

International Symposium on Safety Science and Engineering in China, 2012
(ISSSE-2012)

The Security Risk Assessment Methodology

Chunlin Liu^{a,*}, Chong-Kuan Tan^b, Yea-Saen Fang^b, Tat-Seng Lok^c

^aConstruction Management Department of Tsinghua University

^bK&C Protective Technologies Pte Ltd, 125A #02-132, Toh Payoh Lorong 2, Singapore 311125

^cNanyang Technological University, c/o Protective Technology Research Centre, School of Civil & Environmental Engineering, Nanyang Avenue, Singapore 639798

Abstract

There is an increasing demand for physical security risk assessments in which the span of assessment usually encompasses threats from terrorism. This paper presents a brief description of the approach taken by the author's organization based on a systematic computation of ratings, which are further supported by logical arguments backed by factual data. The procedure compiles the results of the threat assessment, vulnerability assessment and impact assessment to arrive at a numeric value for the risk to each asset against a specific threat given by:

$$\text{Risk Rating}(R) = \text{Threat Rating}(T) \times \text{Vulnerability Rating}(V) \times \text{Impact Rating}(I)$$

This systematic approach could assist decision-makers in selecting risk management strategy by ranking various threats in accordance to their respective Risk Profile. Following which mitigation measures can be explored to reduce the risk for valuable assets, and a logical prioritization for implementation can be achieved.

© 2012 Published by Elsevier Ltd. Selection and/or peer-review under responsibility of the Capital University of Economics and Business, China Academy of Safety Science and Technology. Open access under [CC BY-NC-ND license](https://creativecommons.org/licenses/by-nc-nd/4.0/).

Keywords: Safety Rating, Risk and Threat Assessment, Methodology, Vulnerability, Security

1. INTRODUCTION

There is an increasing demand for physical security risk assessments in many parts of the world, including Singapore and in the Asia-Pacific region. This has arisen for a number of reasons. One is the stake for which economies and businesses have become too critical to be ignored, particularly if a low-cost counter-measure perceived security incident giving rise to devastating consequences. Secondly, economies and businesses increasingly see the need to take due diligence and risk management steps to manage physical security risks and to protect their critical assets, just as they would of other risks such as financial/capital assets.

Physical security risk assessment of threats including that from terrorism need not be a black box art nor an intuitive approach based on experience. Increasingly, rigor is being demanded and applied to the security risk assessment process and subsequent risk treatment plan.

This paper presents a short background study and description of the systematic risk assessment methodology used by the author's organization.

* Corresponding author. Tel.: (65) 62580620; fax: (65) 62586210.
E-mail address: liu.chun.lin@kcept.com.sg

2. CUSTOMISING THE RISK ASSESSMENT METHODOLOGY

Currently, there exist a number of industry publications on the topic of risk assessment. A Reference List is provided which includes some of the best guidelines at the present time. Notably, the publications from Sandia Laboratory Security Risk Assessment and Management [3] and from the Federal Emergency Management Agency (FEMA), which publishes a number of guidelines, are worthy references. A relevant publication is FEMA 426 Reference Manual to Mitigate Potential terrorist attacks against Buildings [4]. In Singapore, the authorities recommend two publications by the local authorities [1-2] which are often cited in risk assessments and risk management solutions.

Based on industry guidelines in the above publications, and coupled with the author's in-house expertise and practical experience, we have developed a systematic risk assessment methodology which is appropriate to Singapore and to the Asia-Pacific region.

2.1. Importance of Risk Assessment

Risk assessment is a crucial, if not the most important aspect of any security study. It is with an accurate and comprehensive study and assessment of the risk that mitigation measures can be determined.

The objective of Risk Assessment is to identify and assess the potential threats, vulnerabilities and risks to which a facility under assessment is exposed to and their impact on its primary services and operations.

Risk Assessment also establishes the basis and rationale for mitigation measures to be planned, designed and implemented in the facility so as to protect the lives of people and to reduce damage to properties against potential threats.

2.2. Methodology of Risk Assessment

There are numerous methodologies and technologies for conducting risk assessment. One approach is to assemble the results of a Threat Assessment, Vulnerability Assessment, and an Impact Assessment to determine a numeric value of Risk for each asset and threat pair.

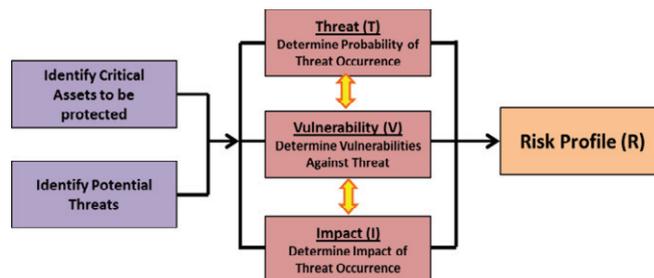


Fig.1 Illustration of Risk Assessment Process

The Risk Assessment methodology introduced herewith employs both quantitative and qualitative techniques to provide findings resulted from a systematic computation of ratings, which are supported by logical arguments backed by factual data. It is based on the methodology used by the Federal Emergency Management Agency (US) [4- 5] and on a similar risk assessment model to mitigate potential terrorist attacks against buildings.

The methodology compiles the results of the threat assessment, vulnerability assessment and impact assessment to arrive at a numeric value for the risk to each asset against specific threat in accordance with the risk formula:

$$Risk = T \times V \times I \quad (1)$$

Where

T = Threat Rating, V = Vulnerability Rating and I = Impact Rating

The entire process of Risk assessment can be summarized as:

- identify the assets and people that need to be protected.
- perform a threat assessment to identify and define the threats that could cause harm to the facility and its inhabitants. Identify assets and threats.
- Conduct a vulnerability assessment to identify weaknesses that might be exploited by a terrorist or aggressor.
- Compute the risk using the results of the asset value, threat, and vulnerability assessments.

2.3. Identification of Critical Assets to be Protected

Prior to conducting a Risk Assessment, it is most important to identify all the critical assets within the facility that require protection.

Assets are resources of value to the facility, which can be tangible (e.g., tenants, installations, facilities, equipment, activities, operations, and information) or intangible (e.g., processes or a company's reputation). In order to achieve the greatest risk reduction at the least cost, identifying and prioritizing the facility's critical assets is a vital. This can be accomplished by defining/ understanding the facility's core functions and processes; and by identifying infrastructures/ components within the facility that are essential to achieving and maintaining such core functions and processes. The details can be tabulated to list these assets and their corresponding redundancy and recovery plans, so that reference can be made in the course of Risk Assessment. Table 1 shows an example of this process.

Table 1 – List of Critical Facilities in the Facility under Assessment

Ref No	Name of Asset	Description of Asset	Redundancy (Quantity & Readiness)	Recovery Plan (Repair/ Replacement Cost & Time)
ASST01	Asset A	e.g. Production system...	e.g. 100% redundancy, but requires 2 hours lead time to fully activate.	e.g. \$10,000 - \$50,000/ 6 months
ASST02	Asset B	e.g. Emergency power supply	e.g. 1 no 2 cells on hot standby	e.g. < \$200,000 / 3 months
ASST03

2.4. Identification of Potential Threats

The preliminary step in the Risk Assessment process is to subject the facility under assessment to a list of threats; and assess the applicability and probability of occurrence of such threats at the facility based on geopolitical situation, current events, and historical data within the region that are relevant to the facility.

In many cases, such a list of possible or potential threats is compiled based on known criminal and terrorist activities within the region where the facility is located. In others, the list may be prescribed by government agencies or the body authorizing such Risk Assessment. Table 2 below shows a list of threats that are commonly used for Risk assessment in, for example, Singapore.

It is important to note that certain threats are peculiar to a particular security environment whilst others can occur at any time under any environment. One common way of defining such different environments within which different levels of threats prevail is to categorize them into Peacetime (PT) and Heightened Security (HS) periods.

- Peace Time (PT) - Time whereby the prevalent security situation is normal both at the national level and the facility level. High-level security threats are not expected to occur. For the purpose of Risk Assessment, it is commonly taken that baseline security measures are in place at the facility.
- Heightened Security (HS) – A period of heightened state of alert as a result of present and lurking aggression from known criminal or terrorist organizations. Heightened Security situation may also be declared when intelligence from government agencies indicates a high risk of terrorist attacks. During Heightened Security period, security measures are expected to be strengthened whilst maintaining general daily routines.

Table 2 – List of Conventional Threat Scenarios (The table below illustrates possible threat scenarios that are commonly considered in Risk Assessments. Actual threat scenarios to a particular facility shall be assessed on a case-by-case basis)

S/No	Threat	Description	Possible Mode of Attack	Applicable During
T1	Theft / Burglary	Unlawful removal of property from the facility during and/or after business hours committed by lone motivated individuals (insiders/outside) or organized syndicates.	Unauthorized access with or without the use of special tools and equipment, including theft of Intellectual Property by Industrial Espionage.	PT HS
T2	Robbery	Removal of valuables by force or threat of force or by fear. May occur during and/or after business hours and may be committed by motivated individual(s) or organized syndicates.	Use of physical force, threat of bodily harm or intimidation of visitors and staff with or without use of weapons (either lethal or non-lethal weapons).	PT HS

S/No	Threat	Description	Possible Mode of Attack	Applicable During
T3	Public Order Incidents	(1) Demonstrations and/or mass protest situations by organized groups in the facility. (2) Incidents involving employees or contractors e.g. labour disputes. (3) Fighting/rioting by unruly persons (4) Drunk and disorderly behavior by individuals	(1) & (2) could include use of projectiles, stones, furniture, loose objects or even inflammable materials Disgruntled employees or contractors causing trouble in the Plant's site / premises to attract attention to their cause.	PT HS
T4	Sabotage / Mischief	Hostile acts to sabotage, damage, destroy or disable operating systems and equipment in the facility. May be carried out by Disgruntled staff, Contractors / workmen who are unsupervised; or external parties who enter premises by unauthorized means; or external elements in collusion with disgruntled staff.	Cutting off electricity, telephone or utility supplies Tampering with computer systems, M&E services, plant and equipment. Cold sabotage with willful neglect of maintenance / services and manipulation of equipment Arson	PT HS
T5	Stand-off Attack with Hand Thrown Devices	Subversive elements launch stand-off attacks using Molotov cocktail or other incendiary devices from outside perimeter.	Small quantities of incendiary devices e.g. Molotov cocktail, thrown from outside the perimeter towards the facility's critical function assets.	PT HS
T6	Explosive Attack with Mail or Parcel Bombs	Sending explosives by normal mail or courier services. Commonly 2kg to 5 kg TNTNEQ are considered.	Concealing explosives inside mail or parcels to particular individuals. The device will explode when the mail or parcel is opened, injuring people or damaging essential equipment in its immediate vicinity.	PT HS
T7	Attack Against High Profile Individuals	Attacks against high profile visitors (politically, diplomatically or commercially important persons, local and foreign dignitaries)	High precision and long range sniper weapons (with up to 1 km range /line of sight) could be used.	PT HS
T8	Placement of Improvised Explosive Devices (IEDs)	Placement of an IED inside the premises. Such attacks may be carried out by subversive elements motivated by political or religious ideology. Commonly 2kg to 20kg TNTNEQ are considered, depending on the profiles of pedestrians accessing the facility.	The IEDs could be concealed and carried by hand in a luggage, a bag or on the body and placed inconspicuously at critical assets. The IED could be detonated by timer, remote control, booby-trap or pressure release trigger.	PT HS
T9(a), (b) & (c)	Attack by a vehicle carrying improvised explosive devices (VBIEDs)	The attack could be carried out by subversive elements who are motivated by political or religious ideology using IED concealed inside a vehicle. Commonly 200kg to 1000kg TNTNEQ are considered, depending on types of vehicles accessing the facility.	(a) Potential adversaries may place IEDs (made of fuel oil, fertilizers and volatile materials) of a specified weight of TNT equivalent (TNT _{NEQ}) hidden inside a vehicle and detonate from a location adjacent to the facility. (b) The vehicle could also park or be left abandoned inside the facility compound and detonate by a timing device or remote control device. (c) The vehicle could also be driven into the premises by forced entry and detonate by a timing device or upon impact.	PT HS
T10	Attack with Chemical / Biological / Radiological Agents	Attack by subversive elements motivated by political or religious ideology to contaminate air supply and water sources via introduction of Chemical/ Biological/ Radiological agents into air-conditioning systems, water tanks etc or via releasing in public.	(a) Chemical Agents - Introduction of Chemical chlorine, nerve agents (e.g. sarin, soman, tabun, VX, etc), blister agents (e.g. sulphur mustard, nitrogen mustard, lewisite, etc), blood agents (e.g. hydrogen cyanide, cyanogens chloride, arsine, etc). (b) Biological Agents - Introduction of bacteria (e.g. anthrax, tularaemia, plague, salmonella, etc), toxins (e.g. botulinum toxin, ricin, etc). (c) Radiological Agents - Release of Cesium-137, Cobalt-60, Americium-241 in public areas as radiological dispersal devices (i.e. dirty bombs)	PT HS
T11	Armed Assailant Attack	Attack by a group of 5-7 adversaries armed with weapons, grenades or incendiary devices to kill, maim or even seize victims as hostages.	Assailants may seize victims in a building or a vehicle / coach as hostages to set demands or propagate political statements	HS

3. Threat Assessment

3.1. Threat Assessment Criteria

The following criteria are designed to assess the likelihood of occurrence of specific threats to a facility. Definition of scores from 1 to 5 (5 being the greatest threat) for each factor are described in Table 5. The average score of the sum of all the seven threat factors will, in turn, derive the Threat Assessment Rating. Refer to definition of rating in Table 5.

Table 3 shows the corresponding Threat Assessment Rating, while Table 4 outlines the Threat Assessment Work Sheet that would be considered in a vulnerability and holistic analysis of the scenario.

Table 5 - Threat Assessment Criteria

(The table below illustrates possible threat assessment criteria that are commonly considered in Risk Assessments. Actual quantification of each criterion to a particular facility shall be established on a case-by-case basis.)

Threat Assessment Factors Matrix							
Score	Access to Resources	Knowledge/ Expertise	History of Threats	Asset Visibility/ Symbolic Value	Asset Accessibility	Site Population	Collateral Damage
5	Readily available	Basic knowledge/ open source	Local incident, occurred less than a year; caused great damage; building functions and occupants were primary targets	Existence widely known/iconic	Open access, unrestricted parking	Less than 1000	Beyond 1km radius
4	Easy to produce or acquire	Bachelor's degree or technical school/open scientific or technical literature	Regional/ local incident; occurred between 1 and 5 years ago; caused substantial damage; building functions and occupants were one of the primary targets	Existence locally known/ landmark	Open access, restricted parking	Less than 500	Within 751m to 1km radius
3	Difficult to produce or acquire	Advanced training/rare scientific or declassified literature	International incident; occurred between 6 and 10 years; caused moderate damage; building functions and occupants were one of the primary targets	Existence publish/well-known	Controlled access, protected entry	Less than 200	Within 501m to 750m radius
2	Very difficult to produce or acquire	Advanced degree or training/ classified information	International incident; occurred between 11 and 15 years ago; caused localized damage; building functions and occupants were not the primary targets	Existence not well-known/ no symbolic importance	Remote location, secure perimeter, armed guards, tightly controlled access	Less than 100	Within 251m to 500m radius.
1	Extremely difficult to produce or acquire	Advanced degree or advance training/ classified information and vast experiences	International incident; occurred between 16 and 20 years ago; caused localized damage; building functions and occupants were not the primary targets	Unaware of existence	Remote location, precipitous terrain, secured perimeter, armed guards, tightly controlled access	Less than 50	Within immediate area to 250m in radius.

Table 6 - Threat Assessment Rating

Threat Rating		
Very High	5	Very High – The likelihood of a threat, weapon, and tactic being used against the site or building is imminent. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is credible.
High	4	High – The likelihood of a threat, weapon, and tactic being used against the site or building is expected. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is credible.
Medium	3	Medium – The likelihood of a threat, weapon, and tactic being used against the site or building is possible. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is known, but is not verified.

Low	2	Low – The likelihood of a threat, weapon, and tactic being used in the region is possible. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat exists, but is not likely.
Very Low	1	Very Low – The likelihood of a threat, weapon, and tactic being used in the region or against the site or building is very negligible. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is non-existent or extremely unlikely.

Table 7 - Threat Assessment Work Sheet

S/no.	Threats	Threat Period / Rating	
		PT	HS
T1	Theft / Burglary	----	----
T2	Robbery	Rating – e.g. 2 (Low)	Rating
		Explanation – e.g. The likelihood of a threat, weapon, and tactic being used in the region is possible. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat exists, but is not likely.	Explanation
T3	Public Incidents	Order	----

	Rating 5 (Very High)		Rating 4 (High)		Rating 3 (Medium)		Rating 2 (Low)		Rating 1 (Very Low)
--	----------------------	--	-----------------	--	-------------------	--	----------------	--	---------------------

4. Vulnerability Assessment

4.1. Vulnerability Assessment Criteria

Vulnerability is defined as any weakness that can be exploited by an aggressor to make an asset susceptible to damage. A vulnerability assessment is an in-depth analysis of the building functions, systems, and site characteristics to identify building weaknesses, sufficiency of existing security measures (if any), lack of redundancy and duration of operation recovery from an attack. Criteria used for conducting a vulnerability assessment are as follows:

- Susceptibility

It concerns with the question of how prone the asset is to the threat due to its attractiveness in terms of its physical and symbolic characteristics and the level of visibility which contribute to asset’s overall weaknesses. Weaknesses are identified through an evaluation of the facility’s environmental, architectural and structural features, security measures and processes. A minor weakness is one that vulnerability is not obvious and even if it is discovered by a perpetrator, it is not easily overcome without the perpetrator being detected. A weakness means that the vulnerability is obvious but not easily overcome by perpetrator without being detected. A major weakness means that the vulnerability is exposed to perpetrator and it is easily overcome without being detected.

- Adequacy of Security

The adequacy of existing protection measures is examined in relation to the specific threats that are applicable to the asset(s).

- Redundancy

The level of redundancy depends on the organization’s fault tolerance and mode of operations. The assessment takes into consideration the geographical distribution and interdependencies of the components of primary service and its back-ups within the facility as well as the availability of alternative work locations or recovery sites for primary service or processes.

- Recovery Periods

Recovery Period refers to the time after the occurrence of a threat or attack to the time when normal / core operations are restored be it at alternative site or alternative mode of business operations.

The criteria by which this vulnerability assessment is conducted and analyzed are shown in Table 6. Table 7 provides the vulnerability rating and the corresponding Vulnerability Assessment Work Sheet is given in Table 8.

Table 9 - Vulnerability Assessment Criteria

(The table below illustrates possible vulnerability assessment criteria that are commonly considered in Risk Assessments. Actual quantification of each criterion to a particular facility shall be established on a case-by-case basis.)

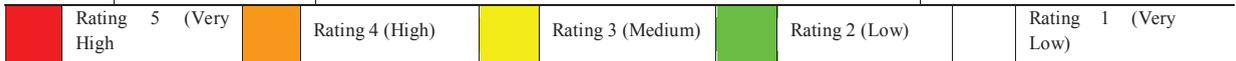
Rating	Susceptibility	Security Measures	Redundancy	Recovery Period
5	One or more major weaknesses have been identified that make the asset extremely susceptible to an aggressor.	Lacks security measures	Lacks redundancies.	Entire facility functional again after 1 month after an attack.
4	One or more major weaknesses have been identified that make the asset Highly susceptible to an aggressor.	Poor security measures	Poor redundancies. 25% of the facility's function can be restored.	Most parts of the facility would be functional again within a month after an attack.
3	A weakness has been identified that makes the asset moderately susceptible to an aggressor	Moderate security measures	Moderate redundancies. 50% of the facility's function can be restored.	Most part of the facility would be functional again within a week after an attack.
2	A minor weakness has been identified that slightly increases the susceptibility of the asset to an aggressor	Good security measures	Good redundancies. 75% of the facility's function can be restored.	The facility would be operational within a day after an attack.
1	Very low susceptibility of the asset to an aggressor.	Excellent security measures	Excellent redundancies. 100% of the facility's function can be restored.	The facility would be operational immediately after an attack.

Table 10 - Vulnerability Rating

Criteria		
Very High	5	One or more major weaknesses have been identified that make the asset extremely susceptible to an aggressor or hazard. The building has no capability of resisting the occurrence of a threat.
High	4	One or more major weaknesses have been identified that make the asset highly susceptible to an aggressor or hazard. The building has low capability of resisting the occurrence of a threat.
Medium	3	A weakness has been identified that makes the asset moderately susceptible to an aggressor or attack. The building has moderate capability of resisting the occurrence of a threat.
Low	2	A minor weakness has been identified that slightly increases the susceptibility of the asset to an aggressor or attack. The building has good capability of resisting the occurrence of a threat.
Very Low	1	No weaknesses exist. The building excellent capability of resisting the occurrence of a threat.

Table 11 - Vulnerability Assessment Work Sheet

S/no.	Threats	Threat Period / Rating	
		PT	HS
V2	Robbery	----	----
		----	----
V3	Public Order Incidents	Rating – e.g. 3 (Medium)	Rating
		Explanation – e.g. A weakness has been identified that makes the asset moderately susceptible to an aggressor or attack. The building has moderate capability of resisting the occurrence of a threat.	Explanation
V4	Sabotage / Mischief	----	----
		----	----



5. Impact (Consequence) Assessment

5.1. Impact (Consequence) Assessment Criteria

An Impact (Consequence) Assessment was carried out to assess the consequences/impact of the probable occurrence of the various identified threats against the facility under assessment. The assessment is based criteria, including Loss of Life, Injuries, Loss or damage of building / assets, Loss of primary service (importance / duration), and Impact on economic and/ or socio-political well-being of the country / nation.

5.2. Qualification of Criteria

Impact assessment in terms of number of life loss and potential number of injuries shall take into consideration the worst case scenario of a full occupancy capacity of the facility under assessment. The criteria of assessing loss of damage building/assets shall consider the construction cost of the building/asset. Assessment on loss of primary service shall be based on the recovery period of re-constructing the building/asset and/or replacement of supporting equipment which determine the operability of the entire facility. Lastly, assessment on impact on economic, political and social well-being of the country / nation is based on the envisage impact, state of preparedness, and perception of the government, as well as the citizens after the news of a potential threat has taken place. It is most important to note that the criteria used here are just for reference. The actual figures used as criteria for every facility under assessment **MUST** be co-developed by the Assessor and the owner/ stake holder of the facility. This is because the threshold of bearing certain impact (or consequence) may vary from organization to organization, and from facility from facility. Refer to breakdown of these criteria in Table 9. Similarly, Table 10 shows the Impact Rating and the corresponding Impact (Consequence) Assessment Work Sheet is given in Table 11.

Table 12 - Impact Assessment Criteria

(The table below illustrates possible impact assessment criteria that are commonly considered in Risk Assessments. Actual quantification of each criterion to a particular facility shall be established on a case-by-case basis.)

S/n	Criteria	0	1	2	3	4	5
1	Loss of life	No Loss of Life	Less than 1% of population	1% to 2% of population	More than 2% but less than 3% of population	3% to 4% of population	More than 4% of population
2	Injuries	No Injury	Less than 10% of population	10% to 20% of population	More than 20% but less than 30% of population	30% to 40% of population	More than 40% of population
3	Loss due to damages to building/ asset	No Impact	Less than 1% of Overall Construction Cost	1% to 2% of Overall Construction Cost	More than 2% but less than 3% of Overall Construction Cost	3% to 4% of Overall Construction Cost	More than 4% of Overall Construction Cost
4	Loss of primary services	No Loss	Less than 1 day	1 day to 1 week	More than 1 week but less than 1 month	1 month to 6 months	More than 6 month
5	Impact on national economic/ socio-political wellbeing	No Impact	Insignificant	Minor	Moderate	Major	Catastrophic

Table 13 - Impact Rating

Impact Rating		
Very High	5	Loss or damage of assets has exceptionally grave consequences, such as extensive loss of life, widespread severe injuries, or total loss of primary services, core processes, and functions; property damage; and a catastrophic impact on economic and political well-being of the nation.
High	4	Loss or damage of assets has grave consequences, such as loss of life, severe injuries, loss of primary services, or major loss of core processes and functions for an extended period of time; and functions; property damage; and a major impact on economic and political well-being of the nation.
Medium	3	Loss or damage of assets have moderate to serious consequences, such as injuries or impairment of core functions and processes; and functions; property damage; and a moderate impact on economic and political well-being of the nation.
Low	2	Loss or damage of assets have minor consequences or impact, such as a slight impact on core functions and processes for a short period of time; and functions; property damage; and a minor impact on economic and political well-being of the nation.
Very Low	1	Loss or damage of assets have negligible consequences or impact; and functions; property damage; and an insignificant impact on economic and political well-being of the nation.

Table 14 - Impact (Consequence) Assessment Work Sheet

S/no.	Threats	Threat Period / Rating	
		PT	HS
C1	Theft / Burglary	Rating - e.g. 1 (Very Low)	Rating - e.g. 1 (Very Low)
		Explanation - e.g. Loss or damage of assets have negligible consequences or impact; and functions; property damage; and a very low impact on economic and political well-being of the nation.	Explanation - e.g. Loss or damage of assets have negligible consequences or impact; and functions; property damage; and a very low impact on economic and political well-being of the nation.
C2	Robbery	Rating	Rating
		Explanation	Explanation
C3	Public Order Incidents	----	----
		----	----

	Rating 5 (Very High)		Rating 4 (High)		Rating 3 (Medium)		Rating 2 (Low)		Rating 1 (Very Low)
---	----------------------	---	-----------------	---	-------------------	---	----------------	---	---------------------

6. Risk Assessment

As mentioned at the beginning of this paper, the methodology of risk assessment is to assemble the results of the Threat Assessment, Vulnerability Assessment, and Impact Assessment so as to determine a numeric value of risk for each asset and threat pair in accordance with the following expression:

$$\text{Risk Rating(R)} = \text{Threat Rating (T)} \times \text{Vulnerability Rating (V)} \times \text{Impact Rating (I)}$$

The values of T, V and I are derived from the respective assessments tabulated in previous sections. To compute the Risk Rating (R), the values of T,V, and I are multiplied. The Risk Rating of the facility against a specific threat will be taken to compare with a Quantitative Risk Range to in turn establish a Risk Profile of the facility against the threat. Security designers, architects and building engineers can then base on such Risk Profile to design mitigation measures against the threat. For example, a facility that is identified to be exposed to High Risk of Vehicle Borne IED (VBIED) threat will have to design the structures, façade, drop-off points, lobbies in a manner that probability, vulnerability, and impact of a VBIED attack is minimized. Table 12 shows the Risk Profile/ Rating of this analysis.

Table 15 - Risk Profile / Rating

Rating	Risk Level	Quantitative Risk Range
5	Very High	91 to 125
4	High	45 to 90
3	Medium	16 to 44
2	Low	3 to 15
1	Very Low	1 to 2

The Risk Assessment Work Sheet below summarizes the entire Risk Assessment exercise. It captures the essential results from the previous 3 Assessments, computes them into the Risk Ratings, and establishes the overall Risk Profile of the facility against a certain threat. Table 13 illustrates how the computation is assembled and formalized in a Work Sheet.

7. Risk Ranking

To help the decision-making process in selecting and prioritizing risk management strategy, the Assessor can also rank the various threats in accordance to their respective Risk Profile. Generally, for threats of Very High and High risk profile, the natural selection is to mitigate the Risk. For threats of Medium risk profile, mitigation measures should be considered base on the principle of “ALARP” (as low as reasonably practicable). As for threats that are of Low and Very Low risk

profile, it is recommended that facility owners and the security designers should evaluate the Residual Risk before accepting them. Table 14 illustrates an example of how the risk ranking helps in selecting risk management strategies.

Table 16 – Risk Assessment Work Sheet

S/no.	Threats Scenarios	PT					HS				
		T	V	I	Risk Rating (T x V x I)	Risk Profile	T	V	I	Risk Rating (T x V x I)	Risk Profile
R2	Robbery	---	---	---	---	---	---	---	---	---	---
R3	Public Order Incidents	e.g. 2	e.g. 3	e.g. 3	18	Medium	e.g. 4	e.g. 5	e.g. 3	60	High
R4	Sabotage / Mischief	e.g. 3	e.g. 4	e.g. 4	48	High	e.g. 3	e.g. 4	e.g. 4	48	High
R5	Stand-off Attack with Hand Thrown Devices	---	---	---	---	---	---	---	---	---	---
	Rating 5 (Very High)		Rating 4 (High)		Rating 3 (Medium)		Rating 2 (Low)			Rating 1 (Very Low)	

Table 17 – Example of Risk Ranking

Index	Threats	Risk Ranking		Risk Management Strategy
		PT	HS	
e.g. R9a	Attack by a vehicle carrying improvised explosive devices (VBIED) in Adjacent Area	High	Very High	To Mitigate the Risk
e.g. R9c	Attack by a vehicle carrying improvised explosive devices (VBIED) - Forced Entry	Medium	High	To Mitigate the Risk
e.g. R10	Attack with Chemical / Biological / Radiological Agents	Medium	Medium	To Consider Mitigation (ALARP)
e.g. R11	Commando-style attack	Low	Medium	To Consider Mitigation (ALARP)
e.g. R1	Theft / Burglary	Low	Low	To Evaluate Residual Risk before Acceptance
e.g. R2	Robbery	Low	Very Low	To Evaluate Residual Risk before Acceptance
e.g. R3	Public Order Incidents	Very Low	Very Low	To Evaluate Residual Risk before Acceptance

8. CONCLUSION

The Risk Assessment presented here analyses the threat (probability of occurrence), the vulnerabilities (weakness of the facility or an asset against the threats) and the Impact (consequences of the occurrence) when such threats occur to ascertain the level of risk for each asset against each applicable threat. It provides security designers, engineers and architects with a relative Risk Profile that defines assets that are at the greatest risk against specific threats. Following which mitigation measures can be explored to reduce the risk for valuable assets with high risk. As it is not possible to completely eliminate risk, and that every project has resource limitations, security designers must gain understanding of facility owners, architects and engineers in the way mitigation measures affect risk; so that decisions on the best and most cost-effective measures to be implemented can be secured to achieve the desired level of protection (risk management) for the facility.

REFERENCES

- [1] MHA, Enhancing Building Security, 2005.
- [2] MHA, Guidelines on Enhancing Building Security in Singapore (GEBSS), 2010.
- [3] Betty E. Biringer, Rudolph V. Matalucci and Sharon L. O'Connor. Security Risk Assessment and Management. John Wiley & Sons, 2007.
- [4] Federal Emergency Management Agency (FEMA). FEMA 426, Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings, Dec 2003.
- [5] Federal Emergency Management Agency (FEMA). FEMA 452, Risk Assessment, A How-to Guide to Mitigate Potential Terrorist Attacks Against Buildings, Jan 2005.
- [6] ISO/IEC 31010: 2009, Risk management - Risk assessment techniques, Edition 2009.
- [7] HB 167:2006, Security risk management.