Physical Security Guidelines for Financial Institutions

TABLE OF CONTENTS

FOREWORD

Since September 11, 2001, the threat of terrorism has increased globally. Governments around the world have stepped up counter-terrorism measures and are coordinating efforts through a combination of legislative, financial and security mechanisms.

Terrorism-related incidents have risen both in frequency and severity and are also occurring in closer proximity to Singapore. The Singapore Government, for its part, has various programmes in place to mitigate the risk of terrorism. They include border control to prevent the entry of radicalised individuals; restrictions on the import of various controlled items including arms, explosives and bomb-making materials; intelligence sharing with Southeast Asia neighbours, and public education on the need to stay vigilant.

The Association of Banks in Singapore (ABS) has also addressed the threat to physical security posed by terrorism and its potential impact to the financial industry. The safety and security of our employees is of utmost importance and we need to ensure that we have contingency plans in place in the event of a crisis that poses widespread systemic risk. On this note, an industry-wide business continuity exercise known as Raffles Exercise is conducted once every three years to test industry-wide cooperation and response to major operational disruptions affecting the financial sector as a result of a terrorist attack. We included various security incident scenarios, such as swarm attacks, hostage situations, bomb threats, vehicular ram attacks etc. These exercises typically involve the relevant stakeholders such as regulators, ABS members and infrastructure provider.

To ensure traction and follow through, a Standing Committee for Physical Security was established in 2017. The committee provides a mechanism for banks to share, collaborate and address the processes for better physical security and emergency responses.

This guideline aims at consolidating and enhancing the Baseline Security Guidelines issued by the ABS in 2013. This updated guideline provides additional guidance to advisories issued by the Ministry of Home Affairs (MHA) on matters ranging from security measures to responses. They also complement the Guidelines on Enhancing Building Security (GEBSS) issued by MHA in 2013. The GEBSS provides comprehensive and specific technical information on physical security measures while the ABS guidelines provide guidance from a functional perspective. Key elements are included and customised bearing in mind the environment and the type of buildings banks typically operate in Singapore.

The ABS encourages members to utilise these guidelines to actively enhance the state of security programmes in buildings they operate from, as well as to create awareness among employees in security responses. They should also engage their landlords or building management to ensure coordinated responses and to proactively participate in relevant security programmes.

Safety and security cannot be compromised. So let us all do our part to protect Singapore, customers and employees.

Ong-Ang Ai Boon, Mrs
Director
The Association of Banks in Singapore

October 2018

INTRODUCTION

The financial service sector comprises over 1,200 financial institutions and is a critical component of Singapore's economy, contributing to about 25 to 30 per cent of the country's gross domestic product growth over the past years. Securing the environment of the financial services sector is a continual and challenging effort. We need to balance between the protection needs of the sector whilst maintaining the conducive and open business environment that has allowed the sector to thrive. Adopting a risk-based approach to developing a physical security programme will enable each financial institution (FI) to manage its security risks and protection needs in accordance with its circumstances and risk appetite whilst maintaining an environment that is conducive for its businesses.

Singapore remains a prime target for criminals and terrorists to launch attacks on various critical infrastructures, with FIs amongst the top targets. Criminals and terrorists target Singapore for its significant role in the global financial industry. FIs in Singapore are typically located in office buildings, retail spaces such as shopping malls and town centres that are typically close to transportation hubs and busy public spaces. Such locations are typically targeted due to the high human density and are perceived as soft targets by terrorists as compared to a well secured government facility.

The levels of protection recommended in this guideline and in the Ministry of Home Affairs (MHA) Guidelines to Enhanced Building Security in Singapore (GEBSS) establish a foundation reference for the deployment of additional protective measures as threat levels increase. However, they do not assume nor recommend that maximum protection is always required as a standard but suggest design considerations and ways of preparing the FIs in enhancing their security posture to meet the threat level when needed. The ABS Guidelines also aim to achieve the same objectives as stated in the Infrastructure Protection Act (IPA) in accordance with the Infrastructure Protection Bill released by the MHA in 2017. These objectives cover the prevention of a successful attack, minimising casualties and effective response and recovery. FIs are advised to review the associated risks (such as loss of life, major business disruption) and apply the necessary controls as appropriate.

The approach in developing an effective physical security programme is based on the following four components:

- **Threat and Vulnerability Risk Assessment**: The process of conducting a Physical Security Risk Assessment and managing of physical security risks through risk identification, vulnerability assessment, impact analysis and risk treatment.
- **Protection**: Protective measures taken to mitigate the identified physical security risks. These measures cover Infrastructures, Systems, People and Procedures.
- **Detection**: The systems and process of monitoring, surveillance, identification and reporting of a security incident or threat information.
- **Response**: Actions taken to contain and mitigate the impact as a result of a security incident and to resolve the incident.

Some useful supplements to this Guideline are listed below:

- MHA GEBSS - www.mha.gov.sg/docs/default-source/others/mha_guidelines_for_enhancing_building_security_in_singapore_2018.pdf
- SPF Video Surveillance Standards for Buildings (VSS) – www.police.gov.sg/resources/prevent-crime/video-surveillance-system-standard-for-buildings#content
- SPF Prevent Terrorism – www.police.gov.sg/resources/prevent-terrorism/security-guidelines

THREAT AND VULNERABILITY RISK ASSESSMENT

Physical Security Risk Assessment (RA) involves the identification of potential threats and assessment of its impact to the organisation with the objective of identifying and implementing appropriate mitigating physical security measures. There are various instances when a RA or Threat and Vulnerability Risk Assessment (TVRA) should be conducted as needed by regulatory or internal requirements. The MAS Technology Risk Management (TRM) Guidelines states that the TVRA aims to identify the physical security threats and operational weaknesses to determine the level and type of protection required. RAs may differ in complexity due to the different types of infrastructure, criticality and scope. The assessment of threats and vulnerabilities will vary depending on factors such as geographical location, multi-tenancy considerations and type of tenants, asset and operational value to the organisation, impact from natural disasters, and the prevailing political and economic climate. The FI should base its RA on various possible scenarios of threats under the MHA Peacetime Threat list which includes theft, explosives, unauthorised entry, external attacks amongst others. RAs should be conducted in key facilities or critical assets such as Data Centres, Headquarter building/office, flagship branches and critical operational areas.

The RA can be a quantitative or qualitative assessment. The stages of conducting a RA include:

1. identifying and prioritising their assets or operations based on the value and criticality;
2. identifying the threat scenarios that are applicable to its operations and assets taking guidance from the MHA Peacetime Threat list;
3. evaluating the vulnerability of the asset or operation due to the identified threats;
4. conducting an impact analysis; and
5. determining the appropriate physical security measures to counter these risks.

FIs should consider conducting a RA of the (re)development of a building or premise; major modification, renovation or alteration arising from an incident or periodically, at least once every five years. A RA may also be required as and when requested in accordance with the various regulatory requirements such as the MAS TRM Guideline or IPA.

Depending on the needs and resources of the FIs, RAs may be conducted either by internal or external security professionals. For RAs involving any critical infrastructures (CI) and High Profile Development (HPDs) that may require the conduct of structural and blast analysis, FIs should consider engaging a qualified Security Consultant / competent person. Guidance on the criteria for determining competent persons or qualified Security Consultants can be referred to MHA. The scope to these RAs may involve technical assessments such as blast effect analysis, structural resiliency studies and developing a security protection plan as per MHA requirements in the IPA.

Subsequent RAs may be performed by assigned security professionals within the FI's organisation. The RA should be a regular security programme in the FI's security policy to ensure that security measures and plans are reviewed and updated to maintain relevance and effectiveness (GEBSS).

1.1 Vulnerability Assessment

A vulnerability assessment refers to the process of identifying and evaluating gaps or weaknesses in the FI's security controls that, if exploited, may result in damage, loss and/or liability for the FI.

During a vulnerability assessment, the existing security controls for the FI's asset are being evaluated for potential security gaps, weaknesses or non-conformance. Vulnerabilities can include deficiencies in security countermeasures, security technology systems, security protection systems and loss prevention programmes for both the building and the FI's tenanted space. They contribute to the severity of damage when an incident occurs.

New vulnerabilities can arise from:

1. New or escalated threat situation.
2. Deterioration/discontinuation of existing capabilities and security systems.
3. New or updated processes/regulations for example new regulations or guidelines from the authorities or new organisational goals.
4. Availability of new or more cost-effective technologies to potential threat actors that were previously unavailable.
5. Major modification, renovation or alteration to the building or adjoining environment.

1.2 Impact Analysis

An impact assessment covers the analysis of the resulting effect or loss to an organisation due to the occurrence of a physical security incident. This resulting effect may be in terms of operational and business disruption, loss of assets and information, cost etc. The impact assessment takes into consideration that different assets, processes or businesses and the assessed level of damage or loss may have different value to the organisation. Impact assessments thus provide an organisation with the ability to appreciate that not all threats pose the same level of risk, and more importantly, it provides a comparative estimate of the relative significance of the threats posed.

In a criticality assessment, criticality is evaluated by studying the impact of consequences associated with the loss or degradation of an organisation's asset in the event of a successful attack, breach or exploitation. The extent of risk impact depends on the likelihood of various threats and vulnerabilities pairing or linkages capable of causing harm to the organisation should an adverse event occur. Some common examples by which consequences may be expressed or measured include financial value/loss; fatalities/injuries; operational downtime; reputational damage; and regulatory impact.

In evaluating the criticality, the following points can be taken into consideration:

1. The value of the asset, activity or function to the FI's operations (tangible or intangible) such as loss of cash or disruption of network to branches or ATMs. Assets shall include but not limited to people, information and property. The asset value is the degree of the debilitating impact that would be caused by the destruction or incapacity of the asset.
2. The time frame or time period that the asset, activity or function may be unavailable before its effects become significant.
3. Impact on brand, image, reputation arising from negative press or diminished standing in the community.

A criticality assessment may be used to determine resource allocation towards protecting assets that are deemed to be more critical in relation to the threats and vulnerabilities faced.

1.3 Evaluating Risk

FIs should perform an analysis of the potential impact and consequences of these risks on the overall business and operations. There are numerous methodologies and approaches to integrating the assessments on threat, vulnerability and impact to determine security risk. An example of qualifying the risks assessed is illustrated in the GEBSS Chart 1: Risk Assessment (Risk = Threat [T] x Vulnerability of critical asset [V] x Consequences of a successful attack [C]).

There is no single definitive approach to risk assessments as choosing a suitable method depends on the FI's risk management strategy, risk appetite and resources among other factors. Regardless of the methods being used to derive the risk evaluations, FIs should be guided by the following principles for an effective RA process:

1. The scope of the assessment should be clearly defined.
2. The insights obtained from the assessments should be comprehensible to all parties involved in the risk management process.
3. The results of the assessment should be actionable such that it delivers meaningful value for its stakeholders.

As a general principle, the RA should be performed on a periodic basis (at least once every five years) to ensure that the organisation remains up-to-date to its security risks, including its threat landscape and the effectiveness of associated security measures.

1.4 Risk Treatment

Risk treatment decisions are driven by tolerance and acceptable risk levels that are unique to each organisation. Care should be taken to ensure that addressing one risk does not create another. FIs should develop and implement risk mitigation and control strategies that are consistent with the value of the assets and their risk appetite level.

Risk mitigation entails a methodical approach for evaluating, prioritising and implementing appropriate risk-reduction controls. A combination of technical, procedural, operational and functional controls would provide a rigorous mode of reducing risks. Physical access control systems of office entrances, visitor management procedures at the building's entrance, deployment of guards at branches are examples of such controls.

As it may not be practical to address all known risks simultaneously or in the same timeframe, FIs should give priority to threat and vulnerability pairings with high risk ranking/rating that could cause significant harm or impact to the FI's operations. The FI should assess its risk appetite for damages and losses if a given risk-related event materialises. The costs of risk controls should be balanced against the benefits that can be achieved.

The FI should maintain a risk register which facilitates the monitoring and reporting of risks. Risks of the highest severity should be accorded top priority and monitored closely with regular reporting on the risk mitigation actions. The FI should update the risk register periodically, and institute a monitoring and review process for the continuous assessment and treatment of the risks.

2 PROTECTION

The physical security counter-measures will vary for each FI depending on its locality, types of assets and operations. For instance, the measures for offices, retail branches and critical facilities such as data centres would differ.

When designing a security concept for the protection of the FI's premises, it is important to consider the related spaces and find the right balance between creating a secure environment and the requirements of the tenanted space. For example, as a shopping mall is open to the public, identifying suspicious characters may be challenging given the diversity of the public as compared to an office building.

With the rising threat of terrorism globally, large and crowded shopping malls are attractive soft targets due to the potential for mass casualties. The associated risks of such an environment should be taken into consideration by the FIs when designing the security protection measures of an asset. As an example, a branch placed in higher risk locations should consider increasing surveillance and detection capabilities or enhancing emergency response plans in anticipation of such incidents.

Typically, FIs operate in different types of buildings and premises. For example, Representative Offices or Support Offices are usually located in commercial office buildings, Retail Banking Branches in retail spaces, and Essential Services in Critical Buildings or Data Centres. FIs in tenanted spaces should be engaged with the building owner or management to understand the building's Security and Safety Design to plan their own security requirements. These requirements are published in the GEBSS and Appendix – Building Management Engagement Guideline of this document.

2.1 Key Concepts - Layered Approach to Physical Security Defence

Protection refers to measures taken to harden or safeguard an asset from loss or damage. As no single protective measure can reduce or eliminate security risk effectively on its own, a protection in-depth approach comprising of the deployment of layered and complementary controls is commonly used in the design and implementation of protection measures.

Building designs that employ layers of security protection to eliminate or limit the possibility of an attack help reduce the need to employ hardening measures across the entire structure and/or in specific vulnerable areas.

The layering of protective measures is typically based on the following concepts:

- Deter – visible measures that dissuade threat activity;
- Detect – measures that provides the identification or annunciation of threat activity;
- Delay/Deny – measures that slow down or impede the progress of threat activity;
- Response – measures that react to and interrupt threat activity.

More information is available in the Contingency Planning and Protective Security Advisories for Workplaces document by the Singapore Police Force.

Factors to consider when planning physical security controls include:

1. Infrastructure and the architecture of the facility, which include perimeter boundaries e.g. fences, boundary walls; building perimeter e.g. ingresses for people and vehicles; internal spaces and rooms e.g. public areas, secured offices and restricted rooms.

2. Security systems and electronic devices such as alarm sensors, access control systems, turnstiles, video surveillance systems.

3. People, security personnel and employee monitoring and managing access controls.

4. Security procedures and security operations including security incident response guidelines.

Each protection measure may be combinations of functions relating to deterrence, detection, delay/denial and response. For example, a CCTV surveillance is primarily deployed as a detective control but may also serve as a deterrent function depending on where and how the cameras are being deployed. Similarly, lightings can serve to deter malicious activity and may also aid the detection of such activities.

A key principle in designing and implementing an in-depth approach to protection is to layer complementary controls such that it increases the attacker's effort for a successful attack or delay its advance so that breaches can be responded to in a timely manner. The general directions presented in the GEBSS are planned according to the following security layers:

1. Deterrence - measures employed are aimed at leading the attacker to think that his attack plan is likely to fail completely or will not achieve the results desired. Examples includes the deployment of an auxiliary police officer in retail banking branches, security guards in commercial buildings, access control and visitor management procedures.

2. Pro-active security:

    a. Pro-active mind-set - to constantly seek out the potential attacker (Detect), and for security personnel or staff to shift quickly from routine to emergency mode (Respond). Training and familiarisation with security procedures reinforces such mind-sets.

    b. Pro-active deployment - external detection for possible approaching threats (Detect & Deter). Examples include security guard patrol and video surveillance with analytics capabilities.

3. Perimeter security - One of the principles of security is the ability to detect a suspected attacker as far away from the building as possible or at a point where the attacker would cause the least amount of damage. Perimeter security is a critical external ring-fencing function and when not effectively utilised, it may cause serious vulnerabilities to a building's security deployment. In many cases, it is the responsibility of the building management to secure the external perimeter. FIs should be mindful of the measures that the building has implemented as part of their overall assessment. Examples include boundary controls to a secured compound, building and shopping mall's main perimeter entrances, and entrances for stand-alone branches.

4. Access control - Access control covers authorisation and rules by which vehicles, personnel and goods may enter a facility. Access control is a very important security feature as most attacks that take place within the facility will cause much more damage and casualties than an attack which occurs outside. Examples of access control include electronic access control systems for offices and branches, bollards, and turnstiles at critical infrastructure such as the Data Centre.

5. Security command and control room - The security command control room is the nerve centre of security operations and should receive and provide vital information to and from the security personnel on shift, and first responders both in routine and emergency situations. The control room is typically managed by the building management or building security team but sometimes forms part of the FI's operation. FIs should be mindful of these procedures as part of their overall assessment and coordination with

the Security Command and Control Room during a security incident or any other emergency.

6. Emergency procedures – Security incidents such as terror attacks can be lethal as they develop at a rapid rate and usually occur with no warning, leading to possible catastrophic results. Time is critical, and the security response must be immediate, automatic and pre-planned. This is achieved through the emergency and evacuation plans. FIs should ensure that enhanced security procedures that address the responses to these scenarios are available, and that are coordinated with the relevant procedures for the building. This provides the assurance that the FI can manage the increased security risks including escalated threat levels beyond business as usual conditions.

The following sections cover the protection measures on structures, systems, people and procedures in reference to the GEBSS. As the nature of their business and operations among the FIs vary, this section focuses on protection measures that are broad-based.

2.2 Infrastructure

A resilient building infrastructure is essential to reduce the vulnerability of the organisation against security threats. Characteristics such as location, environment, natural physical barriers and general infrastructural protection (e.g. stand-off distance) help to provide security to staff and businesses.

Most terrorist attacks appear to be perpetrated by planting an IED inside the building or by a suicide bomber infiltrating into it. Employing external security layers is one of the principles of security to detect a suspected attacker as far away from the building as possible or at a point where the attacker would cause the least amount of damage.

Another major threat relating to the building perimeter is the easy approach of a potential Vehicle Borne Improvised Explosive Device (VBIED) to the external walls and entrance and ramming through them to enter the main building. The main principle in mitigating such a threat, assuming that complete prevention is not always possible, is by installing physical barriers at vulnerable locations to prevent the vehicle from approaching a critical proximity and installing blast mitigation elements on glass facades.

These threats should be taken into consideration by FIs as part of the pre-lease assessment for new sites or incorporated into new constructions where possible. For existing buildings, vulnerabilities should be assessed and addressed for the related risks to be mitigated.

2.2.1 Stand-off Distance

Stand-off distance is the distance between an asset and a threat, and can be achieved by having an effective perimeter line which creates space between the point of an explosion and the building itself. It is the single most important factor when considering the mitigation of the effects of an explosive attack such as VBIED against a building. There is no ideal stand-off distance as it is determined by the type of threat considered, methods of construction and the preferred level of protection. More details can be found in the GEBSS.

Given the scarcity of land in Singapore and the locality of commercial buildings where bank branches and offices are sited; the application of adopting a large buffer zone for stand-off distance might not be practical for most developments. To mitigate this risk, passive enhancement measures such as clear/vehicle-free zones, planter boxes, bollards and/or low screen walls can be deployed.

Where necessary, for critical buildings such as Data Centres, FIs may consider engaging qualified security consultants to review the adequacy of the security measures to mitigate the risks.

2.2.2 Building Perimeter

Buildings should have a well-defined physical perimeter line separating secure and non-secured areas as it is the last defence preventing any threats from approaching within dangerous proximity of the building. This line can be achieved in many ways depending on the protection level required, and the layout of the building.

Where the FI operates in a tenanted space, considerations of perimeter protection of the office building or shopping mall should not be given only to its immediate tenanted boundary of the office space or branch, but also for the overall building where the premise is sited such as the entrances of the shopping mall or office building. For high risk facilities, organisations may consider the use of perimeter protection by utilising fencing or wall barriers. Key considerations such as construct, deployment and height are important when evaluating the use of security fences or wall barriers.

Besides delaying unauthorised entry, perimeter protection measures should serve to dissuade would-be attackers by making it difficult for intruders to overcome without a high chance of failure or detection. Lighting, CCTV surveillance and/ or intrusion detection systems may be deployed to provide additional deterrence and/ or increase the difficulty of breaching the perimeter protection measure.

The extent of perimeter controls should be determined by the FI's security unit based on the vulnerabilities identified from the TVRA conducted; and through close coordination with the building management to enhance the FI's own perimeter control measures.

2.2.3 Entry Points

A physical building perimeter establishes a controlled access area around a building or asset. The number of external entry points including vehicular access should be minimised and appropriately controlled. Depending on the assessed threats, denial/delay measures such as gantries or security gates may be deployed to defend against unauthorised or forced entry. The GEBSS provides the technical standards and guidelines to these perimeter line design and protection measures.

In addition, the use of lighting, CCTV surveillance and intrusion detection systems may be deployed as complementary security measures at entry points. Exterior doors and windows should be of sturdy and fixed construction, with secure locking devices. External glass facades, doors or windows vulnerable to damage may require additional protection such as the use of tempered glass or shatter-resistant film.

The plan to prevent unauthorised entry or to delay intrusion can be developed based on the following considerations:

- Where are the entry points in their building, office, branch and critical facility?
- What are the vulnerabilities of these entry points? For instance, are there multiple entry points with varying degrees of difficulty in monitoring and control? What are the strength of construction and materials used for entry point controls?.
- How can these vulnerabilities be addressed or mitigated? Can turnstiles or gates be installed?

- Who can the FI work with to enhance the security protection plans for entry points? Can the building management and security, or Singapore Police Force's Safety and Security Watch Group (SSWG) provide assistance?

2.2.4 Walls and Partitions

Walls and partitions serve as physical barriers that segregate public areas from non-public or restricted areas and play a major part in the overall protection capabilities of the building. It is an important line of protection against explosions, small arms attack, forced entry and other crime and terror related threats. Ideally, an envelope wall of reinforced concrete should be constructed with segregation between public and restricted areas reinforced with floor to ceiling slab partitioning. This measure can increase the resistance to forced entry into the restricted areas via access under raised floor boards or above the ceiling boards. In addition, security controls such as seismic detectors may be deployed to enhance the detection of intrusions.

There are various construction methods stated in the GEBSS for building structures, which can be taken into consideration during the design phase for new buildings. Depending on the recommendations of the RA and other requirements, a blast shielding wall may be necessary on certain parts of the building as well as a reinforcement of glass facades and structures.

2.2.5 Internal Access Points

All internal access points should be designed with the appropriate level of security, depending on the sensitivity of the area. As with exterior entry points, internal access points should be complemented with other measures such as lighting, CCTV surveillance and door access control hardware (including secure locking mechanisms). Off operational hours security controls should be considered when designing the access controls.

Additionally, access points to restricted or critical areas should be designed with complementary controls such as 2-Factor Authentication (2FA) as well as intrusion detection systems and/ or audible alarm systems. Depending on the risk assessment, specially designed protected entrances such as gates, interlocking systems or portals may be required to delay forced-entry. The GEBSS has recommendations for the different levels of security, namely, Basic, Medium and High.

2.2.6 Special Facilities

2.2.6.1 Vault/Strong Room

A vault or strong room is a room that is designed for the safekeeping of valuables including cash and negotiables. Depending on the valuables kept and containment limits set by the FI, the vault should be constructed to meet the minimum internationally acceptable standards.

Each vault should have a lockable day gate to prevent unauthorised entry during operating hours and a vault door equipped with dual access control devices such as combination lock and key. CCTV surveillance and/ or intrusion detection systems may be deployed to provide additional deterrence and/ or increase the difficulty of breaching the vault perimeter. The intrusion detection system should be monitored to facilitate prompt response to any security alerts or breaches.

2.2.6.2 Critical Equipment Room

Critical equipment is defined as assets that are essential for supporting the facility's operations and includes machines that support electrical power supply, water supply, air supply, communications systems and networks as well as fire protection systems. As these equipment or utilities may be critical to facilitating emergency response in an attack, their destruction could cause harm that is disproportionate to the building's damage from the direct attack. For example, if a fire breaks out from an explosion, the consequences of the fire protection system failure could be higher than the direct impact of the explosion.

Critical equipment should be located away from areas assessed to be of higher risk, concealed and protected. The rooms housing the critical equipment should be built with adequate protection such as CCTV surveillance, door access control hardware and systems and intrusion detection systems among others. In addition, access should be restricted to authorised personnel only.

If these critical equipment rooms are part of the building's infrastructure that are managed and maintained by the building management, the FI should include them in its risk assessment to also assess them as part of the overall infrastructure supporting the FI's security programme.

2.2.6.3 Mailroom

Mailrooms handle the building's mail streams including receiving and storing mails, parcels and delivery items until they are collected or re-distributed. If such rooms are not properly designed and located, it can present a threat to the building and its occupants when mail items are used as a means of chemical, biological, radiological and explosive (CBRE) attacks. For this matter, mailrooms should ideally be located near the entrance to the building or in a separate facility within the building away from critical areas and key structural elements such as the building's structural columns or transfer beams. For safety reasons, mailrooms should also have dedicated air handling units or ventilation system, taking into consideration the design and cost elements.

The area where incoming mail and parcels are being screened should be designed to mitigate blast effects. As mailrooms are high risk areas, the room should be built with adequate protection such as CCTV surveillance and door access control systems. In addition, access to the mailroom should be restricted to authorised personnel only.

In some instances, FIs may not have an in-house mailroom and may receive mail from third party service providers or couriers. They should recognise that they are may be exposed to the same level of threat from incoming mails, and the relevant mailroom security training should be part of the pro-active security to identify and detect such threats for escalation and response.

2.3 Systems

The appropriate deployment of security systems may enhance the FI's protective capabilities on its assets. Security systems are usually used for the following purposes:

- Detecting and providing an element of deterrence against illicit activities and intrusions.
- Warn security personnel of hostile activity and/or breaches of security.
- Monitor activity in sensitive or vulnerable locations.
- Recording activities for future review or investigations.

In deploying security systems, it is important to not rely on a single technical measure. Instead, security systems should be deployed in a manner such that the controls achieve a complementary and layered approach to asset protection.

It is also important to note that security systems have relatively moderate life spans. It is therefore advisable to design the system to enable periodic changes and updates to ensure the operational readiness of the system. In addition, FIs should also undertake the appropriate hardening measures when designing systems to be protected against cyber-attacks.

More information on the design, selection and specification of security systems is available in the GEBSS.

2.3.1 CCTV Surveillance System

A CCTV surveillance system is an integral part of security monitoring as it provides information for investigative work when the need arises. Depending on where and how CCTV surveillance is deployed, it also serves to deter threat actors if they perceive that their actions are being monitored and recorded.

The proper placement of CCTV surveillance devices should be based on the risks identified. Typically, they are deployed at access, remote or vulnerable perimeter points, areas of critical business operations and areas containing high value or critical assets such as:

- Building perimeter.
- Fence line or boundary lines.
- Vehicle access points.
- Building/Branch entrances.
- Building/Branch lobby.
- Vaults.
- Access control points and screening points.
- ATM/ATM lobby.
- Sensitive/restricted office entrance.
- Critical equipment rooms.
- Technology rooms.
- Data halls.
- Security control room.

In addition, it is important to ensure that blind spots are being adequately covered by CCTV surveillance and that the collection, use and disclosure of CCTV recordings must be in accordance with the Personal Data Protection Act (PDPA).

CCTV recording equipment should be kept in a secured facility which is accessible only by authorised personnel. This is to prevent tampering to the equipment settings or video recordings.

If the CCTV surveillance system is part of the building's infrastructure managed and maintained by the building management, the FI should also assess them as part of the overall infrastructure supporting the security programme in its risk assessment.

For more technical information as well as general concepts and design considerations, FIs can refer to the GEBSS and Video Surveillance System (VSS) Standards for Buildings published by the Singapore Police Force.

2.3.2 Door Access Control System

Effective access control ensures that movement is regulated by determining access into specific areas for authorised persons. Maintaining an effective door access control system is a fundamental principle of good access control management.

When designing an effective electronic access control system, the GEBSS recommends the following considerations:

- The number of entrances should be prioritised and minimised.
- The areas with restricted access such as external doors that should be closed to the public.
- The access control system should not compromise the fire protection and safety systems. Electronically controlled doors should be integrated with the fire protection system, for example, to release the secure door for emergency egress in accordance to local fire code. Fail-secure design electronic locks are recommended for such doors.

Access control should be established at all relevant and appropriate entry/ exit points within the organisation such as building entrance, office entrances, and perimeter doors. Stronger access control measures should be deployed at sensitive or critical areas of the office/ building such as cash processing area, safe rooms, sensitive document storage rooms and data halls. This may include the use of two factor authentication (2FA) access controls systems such as card and PIN, or card and biometric, enabling anti-pass back function, and/or utilising interlocking door access controls (or man-traps).

In addition, a good practice is to create security level zoning with role-based access privileges. An example of security level zoning is as follows:

Accessibility Control	Area	Who Can Access
None	Public areas	All employees and public
Limited	Visitors areas	All employees and visitors with names pre-registered with the Security Office
Moderate	Employee common areas/ offices etc.	All employees
High	Restricted areas	Authorised employees

If the access control system is part of the building's infrastructure managed and maintained by the building management, the FI should also assess them as part of the overall infrastructure supporting the security programme in its risk assessment.

2.3.3 Intrusion Detection and Alarm System

Intrusion detection and alarm systems are aimed at detecting and annunciating unauthorised intrusion and/ or forced entry into a secure area. It is important that an effective deployment

of intrusion detection and alarm systems must be complemented with monitoring and response methods.

The intrusion detection and alarm system include a variety of perimeter, internal and external alarm detection/ triggering devices (such as motion detectors, seismic detectors, door contacts, duress buttons). The system is programmed to monitor various parameters, which may include opening of doors, crossing of perimeter line or movement in a defined space. Upon activation, the system will generate a local alarm and/or transmit the alarm signal to a monitoring centre for follow-up response actions. For more technical information, FIs can refer to the GEBSS.

For high risk areas, redundancy for the alarm communication channel should be incorporated in the alarm system. The system should be also equipped with independent back-up power source and a control panel located in a secured area.

If the intrusion detection system is part of the building's infrastructure managed and maintained by the building management, the bank should assess them as part of the overall infrastructure supporting the security programme in its risk assessment.

2.3.4 Preventive Maintenance and Servicing

Preventive checks and service maintenance of security equipment and systems should be conducted regularly to ensure that the performance of these systems and equipment are maintained at an optimum level.

There should be plans to ensure that designated persons use the appropriate systems with proper controls such as user profiles and user rights. These plans should include procedures on the removal and destruction of any data such as CCTV recordings (e.g. the removal or destruction of faulty recorder hard disks by vendors) and guidance on personal data protection.

For security systems managed and maintained by the building management, the FI should assess them to ensure that they are complete, as part of the overall infrastructure supporting the security programme in its risk assessment.

2.4 People

As security is everyone's responsibility, people play a crucial role in protecting an organisation and its assets. People shape the environment and culture to engender a pro-active mind-set, one of the security layers advocated by the GEBSS to promote vigilance against threats and response to security incidents.

2.4.1 Employees

Effective security depends on the behaviour and mind-set of employees. To develop awareness and a heightened security mind-set amongst employees, FIs should have security awareness and training programmes. These programmes should be designed according to the roles undertaken by the employees.

Core components of security training include information on the type of applicable threats and risk issues, how to identify suspicious persons and activity and what is expected of the employees to detect, prevent and respond to potential security issues. Such training can be conducted face-to-face, via online platforms or through exercises, while awareness programmes can be delivered through newsletters, brochures, posters, bulletins or information packs.

2.4.2 Security Officers

A pro-active approach can enhance security while reducing the opportunities for potential attacks. Security officers should adopt a pro-active mind-set to constantly seek out potential attackers and respond to security incidents promptly. Regular relevant training should be conducted to provide security officers with multiple skills to enable them to detect terrorists and pre-attack reconnaissance.

All security officers must be licensed or exempted by the Police Licensing and Regulatory Department and should be screened before they are selected for employment.

Prior to employment, security officers must be appropriately certified through the Security Workforce Skills Qualifications programmes. Upon employment, all security officers have to be continuously trained in security and safety related procedures, including but not limited to, emergency response and evacuation procedures, bomb call/hoax procedures, suspected mail bomb/ article responses, basic initial fact-finding procedures, basic fire-fighting and basic first aid. Security personnel are required to regularly participate in drills and exercises to familiarise themselves with the applicable security procedures and responses for the building.

2.4.3 Mailroom Personnel

As mailrooms are considered high risk areas, all mailroom personnel should be trained on the procedures to identify, respond and escalate any mail related threats and other suspicious items.

If these personnel are outsourced, FIs should ensure that the service provider adequately trains their employees on the necessary procedures and the building's emergency plan for a coordinated response to handle threats.

2.5 Procedures

Procedures provide guidance and operating protocols to manage physical security situations. Some common procedures relating to the management of personnel and electronic security measures are:

2.5.1 Security Standard Operating Procedures

FIs should ensure that a current and updated set of Security Standard Operating Procedures (SOPs) is available. The SOPs should incorporate the building's SOPs relating to the day-to-day security operations management to the management of escalated security incidents. This will ensure that the FI's SOPs complements the building owner's when responding to security incidents.

The SOPs should include considerations for the various threat scenarios assessed in the RA and the different Security Threat Level to plan for the relevant responses and resources required.

2.5.2 Door Access Review

A regular review of door access privilege should be conducted on a regular basis to ensure that the physical access rights of employees are valid. For sensitive or critical areas, the FI should review the door access log records to check for potential access violations or suspicious activities.

2.5.3 Visitor Management

Visitor management procedures involve the identification, management and tracking of visitors. Visitors should be directed to a registration point at the building or office for identification and screening using appropriate photo identification. During the screening process, visitor details should be recorded either into the visitor management system or record book for tracking purposes prior to issuance of visitor passes. Where necessary, visitors should be accompanied by authorised personnel from the organisation.

If the visitor management system is managed and maintained by the building management, the FI should assess them as part of the overall security programme risk assessment.

2.5.4 Guard Tour Management

Procedures on guard tour management ensure a systematic approach to the patrolling of premises and the provision of adequate security coverage within all strategic and vulnerable areas such as entry points, critical equipment rooms, staircases, and service areas. This would include the scheduling of guard tour timings, routes and checkpoints. As a good practice, guard tour frequency and routes should be varied to avoid predictability.

If the guard management system is managed and maintained by the building management, the FI should assess them as part of the overall security programme risk assessment.

3 DETECTION

One of the key elements of a security programme is detection. Detection refers to the monitoring and surveillance of an organisation's immediate physical premises, surrounding environment and assets to identify security incidents prior to or when an incident occurs. An example of detection is the use of perimeter CCTV surveillance to detect intruders attempting to scale a perimeter fence or breach a door. Through early detection, FIs will be able to carry out timely responses to manage the security incident and mitigate its impact.

Detection measures should be in place for both peace-time and heightened security conditions. System detection can involve both on-site and off-site monitoring to achieve a more robust detection outcome.

3.1 System Detection

System detection include the deployment of video surveillance, intrusion detection and access control systems to detect physical threats, illicit activities or intrusions. It warns designated personnel of potential hostile activity and/or breaches of security and aids monitoring of activities in sensitive or vulnerable locations. The recordings from the system can facilitate post investigations or be utilised as data to be analysed as part of security intelligence gathering. Adequate lighting in the exterior and interior of the premises is also important to assist in the identification process upon detection of potential threats. Please refer to Section 2 for more information on the various security systems.

3.2 Monitoring

System detection should be supplemented with active monitoring so that appropriate actions can be taken to respond to detected threats. Monitoring is typically performed by an off-site third party Central Monitoring Station (CMS) or an on-site Security Control Room (SCR)/Security Command Centre (SCC). The CMS and SCC are the nerve centres where the field devices of the detection systems are connected to triggering alerts which provide vital

information for the response personnel in both routine and emergency situations. A typical security control room should contain all of the main operating stations of the security systems installed throughout the facility. To effectively monitor the alerts, the security control room personnel needs to have a clear situational awareness with the ability to prioritise and filter relevant information received from CCTV surveillance and the alarm system so as to effectively differentiate real incidents from false alarms. The SCR should be equipped with an escalation plan to guide the security personnel on actions to be taken when a threat is detected such as who to notify and escalate. Working surfaces should be designed to enable SCR personnel to have a good view of the CCTV monitors. For more information, please refer to SPF's VSS Standards for Buildings and the guidelines on Image Presentation and Real-time Surveillance.

FIs should consider having different escalation plans to suit the different types of premises (i.e., data centre, retail branch, office buildings etc), to detect security incidents. It is important to have detailed escalation and response plans to ensure that appropriate actions will be taken to mitigate the threats upon detection. Please refer to Section 4 for more information on Response.

3.3 Detection Strategies (On-site In-house/Building Management and Off-site Monitoring)

Different detection strategies for on-site in-house/building management monitoring and off-site monitoring could be deployed depending on the criticality of the premises and whether the premises are owned by the FI. For instance, if a FI is the sole tenant or in a fully owned building or a standalone Data Centre, an on-site in-house monitoring security control room could be established to monitor, detect and escalate a security incident. An FI in a multi-tenant premises will likely be dependent on the on-site building management security control room or to establish off-site monitoring either by an in-house security team located in another location or by a third party security vendor.

3.3.1 Detection through People and Assessment

Detection by trained security officers and employees is a useful means to identify suspicious persons, activities and items. The general roles played by security officers and employees are mentioned in Section 2.

Basic security awareness programmes should be implemented to train employees to look out for suspicious persons loitering in the banking hall or office premises and to escalate to the on-duty security personnel or security department. Security personnel and employees should be trained and briefed on the escalation procedures covering who to notify and escalate if there is any security issue in the premises.

Some of the key suspicious behavioural indicators can be found in the Singapore Police Force website:
https://www.police.gov.sg/resources/prevent-terrorism/security-guidelines/identifying-suspicious-persons)

In addition, please refer to GEBSS for more details on tell-tale signs of suspicious objects and the Dos and Don'ts of handling such objects.

3.3.2 Detection Approaches during Peace-time and Heightened/Enhanced Security Conditions

The FIs should develop different detection approaches for peace time and heightened/ enhanced security conditions.

Detection approaches during peace-time are covered in the preceding narrative on security systems such as video surveillance, intrusion alarms and access controls used in conjunction with active monitoring by the security control room or third party monitoring centre. These measures are supplemented by the people in the FI such as on-site security personnel and/or employees to lookout for any suspicious persons or items.

Detection approaches during heightened or enhanced security conditions will be in addition to the peace time security measures depending on the FI's internal risk assessment. The FIs would need to take into consideration if the premises are owned, partially owned or leased. FIs which own or have full control of the premises, could implement increased or enhanced security measures to detect suspicious persons/vehicles during heightened security or as advised by the authorities. These may include limiting entry/exit points (lockdown procedures), deploying of additional security personnel and conducting bags and/ or vehicular checks or screening. Broadcast to employees could also be undertaken to raise their awareness and to mitigate any potential threats.

FIs, in a multi-tenant building, co-location data centre or with limited control of the premises should consider working with the building management to complement their internal security plans with the building management security plans to mitigate any potential threats in a heightened or enhanced security situation.

3.4 Security Intelligence

Intelligence detection consists of tracking, monitoring and reporting of threat information or intelligence on issues that could create risks to the organisation. The provision of timely, accurate and objective intelligence serves to prepare the FI against identified threats and helps to guide security decisions and actions in managing the organisation's risk management approach.

The intelligence cycle which comprises of four phases – planning and direction; information gathering; analysis; and dissemination, provides a broad methodology for threat intelligence.

3.4.1 Planning and Direction

The first phase of the intelligence cycle is the planning and direction stage, which sets the organisation's intelligence priorities.

This phase entails collecting and understanding the requirements regarding the type, depth and priority of the information to be collected and the information collection methods. By fully understanding the requirements, a monitoring plan could then be developed to monitor the threats. An information collection plan may be used to specify and track the progress of the mentioned requirements, including potential information gaps.

3.4.2 Information Gathering

The second phase of the intelligence cycle relates to information gathering or collection. Depending on the intelligence requirements, the required information may be collected from a range of sources including internal and external as well as open and closed sources.

Information can also be gathered through online platforms such as advanced web searches (including websites, blog), Boolean queries (using keywords and combined with operator words), open source alerts (such as RSS feeds or Google alerts), analytic tools (keywords, mapping) and geo-fencing.

Other information sources include media reports, commercial vendor reports, public databases, the law enforcement authorities), foreign embassies, peer organisations and regulators.

FIs are encouraged to participate in national forums and initiatives such as the Safety and Security Watch Group (SSWG) Scheme that provides various platforms for information gathering and sharing.. In addition, organisations may also establish networks with industry peers and obtain regular communication on industry-specific security issues via security or industry related associations. Seminars, conferences or workshops also provide opportunity for gathering insights on security-related issues and to establish networks with subject matter experts.

Where appropriate and relevant, and subject to the FI's policies and guidelines on information sharing, financial institutions are encouraged to share non-sensitive information and/or intelligence with relevant industry peers on a timely basis so that appropriate actions can be taken.

3.4.3 Information Analysis

After the information is gathered, the security department should, based on the organisation requirements, the information is then analysed, identify information of value, placed in the relevant context and used to assess the potential threats and risks to the organisation by the security department.

3.4.4 Dissemination of Intelligence

The dissemination phase includes a communication plan which will identify the relevant stakeholders and senior management to receive the information, how and when the intelligence is disseminated and method of reporting such as email, written briefs and/or with threat maps. As a general principle, intelligence should be disseminated in a timely manner to the relevant stakeholders and senior management to facilitate the initiation of appropriate actions and responses by the organisation.

4 RESPONSE

Response refers to protective actions taken to mitigate a security incident or an emergency, as well as actions taken to react to a physical security threat. All response approaches can be framed into three main phases:

1. Preparation;
2. Incident Response; and
3. Post Incident Recovery.

4.1 Preparation

Preparation is paramount in managing a security incident or emergency effectively. The preparation phase involves developing plans and procedures to deal with the security threats and risk issues that are being identified by the FI. In developing a response plan, FIs should consider assigning roles and responsibilities to personnel as required during an incident,

identifying the points and modes of response activation, developing specific procedural guidance to dealing with the identified threats as well as accounting for assets and people.

The preparation phase also involves working with the relevant stakeholders such as the building management to align operating protocols and procedures. Emergency planning for buildings and office premises must be tailored to different situations. There are numerous physical security measures that can be taken for security and emergency preparedness. These include deploying visible security cameras, motion sensors, security personnel, locking devices and developing a comprehensive security operations plan.

Staff should be trained to increase the level of security awareness. Towards this end, training programmes should be implemented on how to identify and report suspicious persons, items or activities . In addition, staff should also be trained in handling threatening telephone calls or bomb threats.

Regular security-related exercises and drills should be conducted so that employees and role holders are constantly updated and made aware of the various emergency response procedures.

Building management staff should consider conducting a study of vulnerability issues in the structural resiliency of the property and essential utilities. Adequate physical security measures should be implemented to protect the building and mitigating procedures to ensure that their critical business components are sufficiently protected against terror attacks targeting the infrastructure of the premise.

4.2 Personnel Security

Personnel management is a key component in a physical security incident. Effective management of an incident requires all emergency response personnel to be clear of their roles and responsibilities so that they can carry out their various functions swiftly and effectively.

Staff must be accounted for efficiently when an evacuation is activated. The relevant department responsible should have a system or policy to quickly commence accounting for employees when required so that everyone in the organisation is accounted for. Staff needs to be constantly updated and their sentiments and morale managed when a security related incident occurs. The organisation and the Human Resources department should provide the necessary counselling to affected employees if needed.

4.3 Protocols

Protocols such as SOPs, emergency plans and guidelines help the organisation to be organised and better prepared to face any security incident. These normally involve developing and implementing policies and SOPs related to physical security incidents. Creating staff awareness and training on physical security programme are important to ensure that all protocols and relevant information are disseminated to the relevant staff. To further augment these efforts, regular security simulation exercises should be conducted to strengthen these protocols by identifying and addressing gaps, if any, in these plans.

4.4 Incident Response

Swift action is required to mitigate any damage arising from incidents. Roles, responsibilities and actions to be taken should be clearly defined. This should include coordination and liaison with the relevant external authorities if an incident is escalated.

The incident respondent or Emergency Response Team should first identify the cause of the incident or breach and ensure that incident is contained. This prompt action ensures that measures are taken to mitigate further impact and avoid any inadvertent compromise of the integrity of any follow up investigation.

Response protocols for individuals in the following situations should be developed and simulated:

- Active Assailant
- Bomb Threat
- Mail Delivered Threats
- Chemical, Biological and Radiological Threats
- Person-Borne Improvised Explosive Device (PBIED)
- Vehicle-Borne Improvised Explosive Device (VBIED)
- Hostage Situation

Please refer to the SG Secure website https://www.sgsecure.sg) for more information.

4.4.1 Active Assailant

The guiding principles for individuals to respond to an active attacker threat are “Run, Hide and Tell”:

1. **Run** when it is safe to do so:
   - Consider the safest route.
   - Move quickly and quietly.
   - Stay out of view of the attackers.
   - Insist others leave with you.
   - Leave your belongings behind.

2. **Hide** if you can’t run:
   - Find cover from the attacker and stay out of sight.
   - Lock yourself in but do not get trapped.
   - If you are unable to lock the doors or entrances, place objects such as tables and cupboards behind the doors or entrances to prevent access by attackers.
   - Move away from the doors.
   - Be very quiet and switch your mobile devices to silent mode.

3. **Tell** the Police when it is safe to do so
   - Give your location and where you last saw the attackers.
   - Provide details about the attackers.

4.4.2 Bomb Threat Call

When a bomb threat is received:

1. Do not panic. Stay calm.
2. Alert someone to call the Police. Keep the caller occupied by talking as long as possible while the Police traces the call.
3. The officer receiving such calls should threat them seriously and immediately try to determine:

- the precise location of the bomb and exactly how it looks like;
- the detonation time and what will it set off;
- the amount and type of explosive used; and
- the reason for such an act.

4. It is also important to take note of the following:
   - the caller's voice and vocal characteristics (e.g. pitch, male/female, adult/child);
   - the language used and accent (e.g. local or foreign);
   - manner of speaking (e.g. rapid, deliberate, emotional, angry);
   - background noises (e.g. traffic, music, public announcements, shouting);
   - the person or authority whom this message should be conveyed to;
   - do not antagonise or taunt the caller in any way; and
   - be polite and remain calm.
5. Do not spread rumours.
6. Depending on the situation, evacuation or invacuation response may be annunciated. Follow the procedures as applicable.

4.4.3 Mail Delivered Threat

Bombs/explosives can be delivered through the postal service or courier. Most bombs are designed to detonate when the outer wrapping is cut open or torn. If you receive a mail item such as a letter/parcel suspected of containing explosives, do not attempt to open it but instead take the following actions:

1. Call the Police.
2. If you are not sure of the origin of the mail item but have reasons to suspect that it is a bomb, treat it like a bomb and alert the Police.
3. Place the suspected mail item in a corner of the room away from windows.
4. Evacuate the room and building if necessary, leaving all the doors and windows open. This is to allow the blast if any, to vent and mitigate the harmful effects of the shattering glass.
5. Instruct all personnel and evacuees not to touch anything that looks suspicious while securing the premises.
6. If an explosion occurs and evacuation is affected, give appropriate instructions to re-direct the evacuees to safer/alternative routes of escape.

4.4.4 Chemical, Biological, Radiological (CBR) Threat

If an item is suspected of containing CBR material, the individual should take the following actions:

1. Do not handle the letter or package suspected of contamination. Do not shake or empty the contents of the article.
2. If any of the contents (e.g. powder) is spilled from the article, do not try to clean it up. Quickly, cover the area where the powder was spilled with a suitable item (e.g. clothing, paper, trash-can, etc) to prevent it from spreading. Do not remove this cover.
3. Switch off nearby fans or ventilation units in the proximity of the affected area.
4. Leave the room and close the door or block-off access into the area to prevent others from coming close to the affected area.
5. Wash your hands with soap and water to prevent further spreading of the powder.

6. Remove contaminated clothing as soon as possible and put them in a plastic bag or a suitable container that can be sealed and have them available for the Police/Singapore Civil Defence Force.
7. Shower with soap and water as soon as possible. Do not use bleach or other disinfectants on your skin.
8. List the names and contact numbers of all the persons who were in the room or area, especially those who had direct contact with the powder. Give this list to the Police for follow-up investigations and the issuing of appropriate medical advice/follow-up for individuals who had contact with the powder.

4.4.5 Person-Borne Improvised Explosive Device (PBIED)

PBIEDs are explosives that are concealed on-person, either under or within clothing, shoes, or other types of apparel and can result in mass casualties if detonated in crowded areas. When posed with a PBIED, the individual should:

1. Stay calm.
2. Crawl under a sturdy table or a solid object if things are falling around you, and remain there as long as it is safe to do so.
3. Stay away from glass or fixtures, like windows, mirrors, cabinets, and electrical equipment.
4. Follow the orders of the Police or safety personnel. If an evacuation is ordered, leave the building as soon as you can.
5. Do not go near fire hazards.
6. Once out of the premises, keep as far away from the building as possible.
7. Do not use elevators.
8. The best place to be in an event of an explosion is to stay flat on the ground.

4.4.6 Vehicle-Borne Improvised Explosive Device (VBIED)

A car bomb, lorry bomb, or truck bomb, also known as a vehicle-borne improvised explosive device (VBIED), is an improvised explosive device placed inside a car or other vehicle and detonated. The individual should take the following actions in a VBIED situation:

1. Stay calm.
2. Hide behind a solid object or wall and remain there for at least few minutes as there may be a secondary blast.
3. Stay away from glass or fixtures, like windows, glass panel or doors or electrical equipment.
4. Do not use your mobile phone.
5. Follow the orders of police or security personnel.
6. Keep far away from the blast as possible.
7. If you are injured stay flat on the ground and wait for medical help.

4.4.7 Hostage Situation

Hostage situations can happen at any time, anywhere. The element of surprise and unpredictable nature of these attacks make them one of the hardest situations to prepare for. If you are taken hostage:

1. Remain calm, be polite and cooperative.
2. Do not try to be a negotiator.
3. Speak only when you are spoken to and in a normal manner.
4. Comply with all orders and instructions.
5. Do not make sudden bodily movements, pass comments or cast hostile looks at the captor(s).
6. Carefully observe the captor(s) and memorise physical traits, voice pattern, clothing and other details that will help the authorities.
7. Stay low to the ground or behind cover from windows or doors if possible

4.4.8 Post Incident Review

In the post incident review, FIs are to analyse the root cause(s) and identify gaps in incident responses and vulnerabilities in the physical security plan.

Parties involved in the incident response may want to conduct a self-assessment of their performance and response gaps. Inputs from stakeholders should be sought and used to assess the effectiveness of protocols and identify the scope as well as need for future awareness training.

FIs may conduct a physical security risk assessment as part of the post incident review to identify improvements in physical security systems and infrastructure.

Plans should be developed and implemented to ensure that corrective actions are taken to address the identified gaps and enhancements to the security measures. These lessons learnt should be incorporated into your policies and procedures.

APPENDIX

BUILDING MANAGEMENT ENGAGEMENT GUIDE/CHECKLIST

This Guide/Checklist is intended to assist FIs in engaging building management/owners to have an understanding and an appreciation on the level of physical security preparedness implemented by the building management. It is not intended to be a security risk assessment or to replace any proprietary assessment used by the FIs. Members should engage trained security professionals when conducting a TVRA.

For details on security measures, references may be made (but not limited) to the GEBSS and Contingency Planning and Protective Security Advisories for Workplaces.

Communications between building security and tenants is vital in an emergency and occupants of a building should be made aware of and briefed on emergency security responses. One such channel is through the engagement with agencies such as the Singapore Security & Safety Watch Group (SSWG) of the Singapore Police Force (SPF) for ongoing and emergency communications. FIs which are not direct members of the SSWG should ensure that their building management is. These FIs should receive SSWG communications via the building management as appropriate.

In addition, FIs should have the key contact information of the building such as the emergency contact number or the security control room number.

Getting Started

Before going through this Guide/Checklist, it is recommended to understand the security threats that general buildings are exposed to. They are but not limited to:

1. Unauthorised Entry
2. Improvised Explosive Device (IED)
   a. Vehicle-Borne Improvised Explosive Device (VBIED)
   b. Person-Borne Improvised Explosive Device (PBIED)
3. Bomb Threats
4. Suspicious Articles
5. Armed Attack
6. Chemical, Biological, and Radiological (CBR) Agents

Understanding Building Security

1. Is the building classified as a “critical infrastructure” or “High Profile Development” under the Infrastructure Protection Act purview? If the answer is “No”, proceed to Question 4.

Observations/ Notes:

2. Does the building management engage a designated security manager to manage the security of the building and perform the applicable risk assessments?

Observations/ Notes:

3. Does the building management have a programme to periodically perform TVRAs/Physical Security Risk Assessments?

Observations/ Notes:

Physical Security - Building Perimeter

4. Has the building management assessed the perimeter to be equipped with adequate security measures to detect/monitor intrusions at access points (such as the deployment of CCTVs or intrusion detection devices)?

Observations/ Notes:

5. Has the building management assessed the perimeter to have sufficient lighting to deter and detect intrusion?

Observations/ Notes:

6. Has the building management assessed the perimeter glass façades /windows to be protected against physical attacks?

Observations/ Notes:

7. Has the building management assessed that all the exterior doors are protected against forced entries?

Observations/ Notes:

8. Does the building management have measures to protect the pedestrian drop-off lobby/ driveway against vehicle ramming into the lobby (such as bollards)?

Observations/ Notes:

Physical Security - Car Park and Loading Bays

9. Has the building management assessed the car park and loading bay to have sufficient lighting to provide surveillance, and a safe and secure environment within the mentioned areas?

Observations/ Notes:

10. Has the building management assessed the car park and loading bay to have adequate security measures to detect unauthorised/suspicious vehicles/ persons at?

Observations/ Notes:

11. During heightened security conditions, are there enhanced security procedures to provide additional screening for threats such as VBIEDs for both car parks and loading bay entry points?

Observations/ Notes:

Physical Security - Pedestrian Entrances/Exits

12. Has the building management assessed lighting to be sufficient to provide surveillance, and a safe and secure environment at entrances and lobbies?

Observations/ Notes:

13. Has the building management assessed that there are adequate measures to detect unauthorised/ suspicious persons at the pedestrian entrances/ exits?

Observations/ Notes:

14. During heightened security conditions, are there enhanced security procedures to provide additional screening for physical threats such as weapons or PBIEDs at entry points?

Observations/ Notes:

Physical Security - Security Control Room

15. Are the CCTVs monitored by the security personnel?

Observations/ Notes:

16. Are the security personnel in the security control room able to communicate with the field security officers including the building management staff?

Observations/ Notes:

17. What is the CCTV video retention period and is it assessed to be sufficient?

Observations/ Notes:

18. Is there a regular maintenance programme to ensure that the CCTV systems are operational (such as quality of image, recording, approved field of view is not altered)?

Observations/ Notes:

19. Are the essential equipment (such as Electronic Control Systems, CCTVs recorders, network switches, PA systems & etc.) for security monitoring available during utility (such as power and communications) interruptions?

Observations/ Notes:

Physical Security - Security Personnel

20. Are the security personnel from a PLRD licensed security agency?

Observations/ Notes:

21. Is the training programme for the security personnel deployed assessed to be adequate in equipping them with the relevant skills to perform the duties (as per the SOPs) required to respond to the threats listed in the “Getting Started” above?

Observations/ Notes:

22. Is there a programme where the security personnel are regularly tested for competency in managing security incidents (such as exercises or drills)?

Observations/ Notes:

23. During heightened security conditions, are there any additional security personnel deployed at various ingress and egress points of the building to perform the enhanced security SOPs such as screening?

Observations/ Notes:

Enhanced Security Procedures - Building Management Communication

24. How does the building management communicate to tenants on the current or new security measures/procedures of the building?

Observations/ Notes:

25. How does the building management communicate to the relevant government agencies such as Singapore Police Force, and share relevant information to neighbouring buildings of an occurring security incident?

Observations/ Notes:

26. How does the building management communicate to tenants during a security incident?

Observations/ Notes:

27. How does the building management communicate to tenants on the increase in security threat level or any imminent threat of a security incident?

Observations/ Notes:

28. How does the building management notify tenants to evacuate/lockdown the building in the event of a security incident?

Observations/ Notes:

29. What is the communication protocol to tenants when the building security status returns to normalcy?

Observations/ Notes:

Response Actions

30. Are there training programmes or briefings to educate tenants in detecting, reporting and responding to security incidents (such as those listed in the “Getting Started” section)?

Observations/ Notes:

31. Has the building management’s SOPs catered for mass casualty incidents such as the management of resources to continue to provide security for the building management of the tenants including the liaison with local authorities?

Observations/ Notes:

Evacuation & Invacuation (Shelter-in-place) Procedures

32. Has the building management established evacuation and invacuation procedures for tenants in the event of a security incident?

Observations/ Notes:

33. For the evacuation and invacuation routes, are considerations given to divert tenants away from the suspicious package/object/vehicle?

Observations/ Notes:

34. Does the building management have a minimum evacuation distance for different sized suspicious package/object or a suspicious vehicle?

Observations/ Notes:

35. Are there alternate assembly areas (including virtual assembly areas) if it is assessed that the primarily assembly area is exposed to a similar threat?

Observations/ Notes:

36. If the bomb/PBIED/VBIED/biological threat is in the vicinity (which does not warrant an evacuation) and within the building, does the building management have procedures to secure the building until the local authorities clear the threat?

Observations/ Notes:

Security Threats - Unauthorised Entry

37. What are the response actions by the building security personnel when a tenant reports an unauthorised entry incident?

Observations/ Notes:

38. Does the building have procedures to verify that only authorised personnel are permitted to access the controlled areas beyond the public spaces?

Observations/ Notes:

39. Are visitors registered and screened before permitting access to the controlled areas beyond the public spaces?

Observations/ Notes:

40. Does the building have procedures to limit the number of ingress/egress points and perform security screening during a heightened security situation?

Observations/ Notes:

Security Threats - Improvised Explosive Device

a) Vehicle Borne Improvised Explosive Device

41. What are the response actions by the building security personnel when a tenant reports a suspicious vehicle?

Observations/ Notes:

42. Are the building security personnel trained to assess and identify a suspicious vehicle?

Observations/ Notes:

43. Are there procedures to cordon off the area where the suspicious vehicle is located including the communication to tenants and visitors?

Observations/ Notes:

44. If the threat is real, is there a systematic evacuation procedure for the building?

Observations/ Notes:

45. Does the building management have a minimum evacuation distance for a suspicious vehicle?

Observations/ Notes:

Security Threats - Improvised Explosive Device

b) Personnel Borne Improvised Explosive Device

46. Are the building security personnel trained to assess and identify a suspicious person with PBIEDs?

Observations/ Notes:

47. Are there procedures to cordon off the area where the suspicious person is located including the communication to tenants and visitors?

Observations/ Notes:

48. If the threat is real, is there a systematic evacuation procedure for the building with routes away from the threat?

Observations/ Notes:

Security Threats - Bomb Threat (call or delivered note)

49. Does the building management have a bomb threat checklist and an escalation procedure for tenants that include the emergency contact details during a bomb threat?

Observations/ Notes:

50. Does the building management have a procedure to cordon off the suspicious package/object when assessed to be a threat?

Observations/ Notes:

51. Does the building management have a systematic evacuation procedure if the threat is assessed to be credible (such as isolated zoned announcements for the affected floor and two floors above and below)?

Observations/ Notes:

Security Threats - Suspicious Articles

52. What are the response actions by the building security personnel when a tenant reports a suspicious article incident?

Observations/ Notes:

53. Does the SOP include an assessment of the suspicious articles (such as baggage, mails or parcels) and an escalation process?

Observations/ Notes:

54. Is there a process for the cordoning and isolating the suspicious article?

Observations/ Notes:

55. If the article is suspected to contain a biological threat, are there procedures to isolate and quarantine individuals in contact with the article and perform infection control measures (such as the rinsing/ washing of hands)?

Observations/ Notes:

56. If assessed that an evacuation is required, is there a systematic procedure as listed in the “Evacuation Procedures” above?

Observations/ Notes:

Security Threats - Armed Attack

57. What are the response actions by the building security personnel when the tenant reports an armed attack incident in the vicinity of the building or within the building?

Observations/ Notes:

58. Does the building management have lockdown procedures such as having the elevators homed to the 1st floor, securing all perimeter doors of the building?

Observations/ Notes:

59. Are the tenants advised to remain indoors practicing the “Run/Hide/Tell” procedures?

Observations/ Notes:

Security Threats - Chemical, Biological and Radiological (CBR) Agents

60. Are the tenants trained and briefed on In-Place Protection Plan (IPP) for the building as well as the preparations required of the tenants?

Observations/ Notes:

61. What are the response actions by the building security personnel when tenant reports a CBR incident?

Observations/ Notes:

62. Does the building management have lockdown procedures such as the sealing/closing of ingress/egress points and shutting of fresh air ventilation vents?

Observations/ Notes:

63. Does the building management have a communication procedure to notify the tenants on the activation of the IPP?

Observations/ Notes:

- End -