

1.3 Key Roles & Responsibilities

Most hotels have similar roles that need to be filled. While a larger hotel may dedicate an entire department to one area, smaller hotels typically have a single individual filling multiple roles.

But regardless of the scope of their responsibilities, every individual plays an important part in working together with other departments to create a safe, secure environment for other employees and guests.

In the following section, recommended preventive measures have been grouped according to the following roles, to enable hotels to identify applicable learning points.



Senior Management

Responsible for making business decisions for the hotel.

- Chief Executive Officer
- General Manager
- Hotel Owner

Security Personnel

May consist of hotel employees, external contractors, or a mix of both. They oversee overall safety policy and site security.

- Security Director/Manager
- Security Team
- Company Emergency Response Team (CERT)



Non-Security Operations

Most likely to interact directly with guests. They may fill roles ranging from receiving guests to cleaning, and maintenance.

- Reception and Front Desk
- F&B Department
- Housekeeping Department
- Engineering Team

Hotel Administration

Generally supervisors and administrators who may be responsible for hiring employees or watching over their training and duties.

- Human Resource Department
- IT Department
- Finance Department
- Marketing & Sales Department
- Revenue Management



The list is not exhaustive and may vary across hotels.

2.1 Simple Steps That All Hotels Can Take

As part of the SGSecure@Workplaces programme, hotels can appoint and register SGSecure reps, utilise digital resources on the MOM website, and download the SGSecure Mobile App to stay updated on terrorism-related news, advisories and initiatives. Every hotel, regardless of size, is encouraged to take these steps.

Appoint and register an SGSecure rep

The SGSecure rep should champion SGSecure in peacetime, and be the point of contact between your hotel and authorities during crises. You may register an SGSecure rep below, and find out more about their roles and responsibilities.



Scan QR code
to register your
SGSecure rep

Encourage employees to access and utilise MOM SGSecure@Workplaces educational resources

Access MOM bulletins, videos, briefing slides, lesson plans, brochures, posters, templates, case studies and guides from the **MOM SGSecure@Workplaces** website. Share these self-help tools with employees and colleagues to prepare the workforce, protect the workplace and partner the community.



Scan QR code to access
SGSecure@Workplaces
digital resources

Encourage employees to download the SGSecure Mobile App

The app will allow you to receive important alerts in the event of a major emergency, make 999 calls or alert the Police via SMS.



2.2 Preparing Your Workforce

A prepared workforce consists of vigilant, alert and capable employees who can act on signs of terrorism as soon as they appear. By establishing good practices in hiring, training, and day-to-day operations, hotels can equip employees with the tools and knowledge they need to identify and address possible threats.

Policies and Procedures



Match Your Manpower Needs

Watch out for the symbols below to see how you can adapt a policy to suit your hotel:



Solutions that require few people to implement



Solutions that hotels with more sizeable teams may consider



Senior Management

Appointing Key Personnel

- ☐ Appoint dedicated individual(s) to coordinate and oversee the planning and implementation of security-related activities
- ☐ Appointed individual(s) should receive the necessary training to deal with security incidents before arrival of the Police
- ☐ During a security incident, all employees should know that they must take instructions from the appointed individual(s) before the Police arrive



Hotels with less manpower, or that lack a dedicated security unit, may appoint an individual such as their SGSecure rep, Senior HR Manager or General Manager to take on such duties



Larger hotels with bigger teams may dedicate an Interdepartmental Stakeholder Group to this area

General Procedures

- ☐ The hotel owner should be responsible for the **Emergency Response Plan (ERP)**
- ☐ The ERP should be updated and reviewed regularly, and employees should be familiarised with its contents
- ☐ Regular testing, table top and emergency exercise should be conducted to validate its effectiveness



Security Personnel

Manpower Deployment

- ☐ For general preparedness, ensure that a sufficient number of personnel are always on duty or on call
- ☐ Ensure that personnel are familiar with the hotel's security and emergency plans
- ☐ Formulate a search plan to guide search efforts during a crisis
- ☐ Appoint someone who is familiar with the hotel layout to be in charge of the search team
- ☐ Organise a **Company Emergency Response Team (CERT)** which will be the first line of response in the event of a crisis



Per SCDF guidelines, the minimum configuration for an effective CERT is a Site Main Controller, a Site Incident Controller, and four Emergency Response Team Members (these individuals should undergo mandatory CERT training and at least four members must be first-aid trained)

General Procedures

- ☐ Establish standard operating procedures for various types of terror and cyber attacks
- ☐ Consider involving local authorities or external auditors when conducting a drill or tabletop exercise so that gaps can be addressed to strengthen your hotel's security practices



You can start by focusing on the more common forms of attacks, especially those that small and economy hotels are more vulnerable to



Consider having a more comprehensive set of procedures and tailoring them to your hotel's guest profiles, location and other factors

☐ **Planning process:**

- Consult third-party professionals when evaluating the hotel security plans
- Stay updated on the national terrorism threat assessment released by the Ministry of Home Affairs and tailor security plans accordingly

☐ **Provide security personnel with the following:**

- Easy access to guides or resources about your hotel's procedures to handle terror or cyber attacks
- Regular practices and drills on what to do in an emergency
- Knowledge on how to handle suspicious individuals

Handling Third-Party Contractors

- ☐ Brief them on the hotel security and emergency plans
- ☐ Ensure they are familiar with and have access to the emergency or key contacts
- ☐ Provide them with access to the reporting channel for suspicious activities
- ☐ Have a system in place for screening your contractors' access rights to the hotel premises where appropriate



Non-Security Operations

General Procedures

- ☐ Brief employees on procedures to handle lost employee passes and room keys
- ☐ Learn to spot common tell-tale signs of terrorist activity (see page 58)
- ☐ Stay alert to suspicious items or behaviour when cleaning rooms or working onsite



Hotel Administration

Appointing Key Personnel

- ☐ Establish an on-ground security team staffed by experienced and meticulous individuals
- ☐ The security team can consist of in-house security, contract security, or a combination of both.
- ☐ **Employers may consider the following factors to identify and hire suitable individuals:**
 - Compatibility with your hotel's corporate culture
 - Familiarity with operations
 - Duration of hire (for contract employees)
 - Pre-existing knowledge, skills or specialised training



Tip

There are SkillsFuture and WSQ training courses available to upgrade the skills of your employees (see page 68)

- ☐ Appoint a well-trained employee or a team to oversee information and cyber security



If you are managing your own hotel's cyber security, you can tap on subsidised SkillsFuture courses to upgrade your IT and cybersecurity skills and knowledge



For larger organisations, experienced IT managers should be hired to maintain and operate IT infrastructure, as well as implement security policies

General Procedures

- ☐ **Hiring new employees:**
 - Check and verify the details they provide on their CV or resume
 - Incorporate physical security and cybersecurity training into employee orientation or on-boarding programmes

□ Training current employees:

- Conduct regular checks on security personnel and employees with access to confidential information
- Develop structured training programmes to address specific situations that different segments of employees may encounter
- Instil security awareness in employees through regular refresher courses, and enforce attendance by maintaining records
- Use subsidy and support schemes to cover training course fees and absentee payroll for Singaporean employees



If your hotel qualifies as an SME, you may also be eligible for enhanced training subsidies for SkillsFuture Singapore courses (see page 68)

Safeguarding Your Business

- Establish Crisis Communication Channels for hotel personnel, hotel guests, and third parties to report suspicious events
 - **For employees:**
 - Use mobile messaging applications to create group-based communication and reporting channels
 - Create a call and contact directory of stakeholders (e.g. key employees, hotel partners, etc.) to notify in an emergency
 - **For hotel guests:**
 - Consider creating an emergency hotline for guests to contact in the event of a crisis
- Provide key personnel with two-way communication devices and training to facilitate crisis communication

Day-to-Day Operations

The effectiveness of your hotel security rests on the abilities, awareness and knowledge of the people enforcing it. Constantly reminding employees of correct procedures and staying alert to suspicious behaviour can go a long way in guarding against terror or cyber attacks.



Security Personnel

Handling Third-Party Contractors

- Familiarise employees with authorised third parties
- Verify the identity of unfamiliar or suspicious individuals
- Have a location to detain and question suspicious individuals



Non-Security Operations

General Procedures

- ☐ Put up relevant posters at areas where employees commonly gather (e.g. employee cafeteria or rest areas)
- ☐ Test employees regularly on possible signs of terrorism (see page 58)
- ☐ Conduct drills with Security Personnel on how to act in a crisis



Hotel Administration

General Procedures

- ☐ Remind all employees, regardless of role, to **immediately** contact emergency or key security personnel on spotting suspicious items, activities or behaviour of guests, or weaknesses or lapses in site security
- ☐ Remind all employees to watch for signs of possible radicalisation in colleagues and employees (see page 59)

Cyber Security Practices

- ☐ If there are no dedicated cybersecurity employees, hotels should partner or subscribe to a certified managed security service provider to monitor and respond to cyber incidents and secure computers and networks
- ☐ Ensure employees with access to sensitive information practise good cyber hygiene and data protection habits, such as:
 - Shredding unwanted documents with confidential data
 - Strengthening password security and monitoring of IT assets
 - Installing software to detect and prevent unauthorised access
 - Being able to recognise and report phishing or scam emails
 - Making use of multi-factor authentication for login systems

Illustrated Summary: Preparing Your Workforce



Senior Management

- Assign a person or team to plan and organise security operations
- Regularly review and update ERP*



Hotel Administration

- Consider incorporating security training into the employee orientation programme
- Ensure employee with access to sensitive data practise good cyber hygiene and data protection habits
- Provide key employees with two-way communication devices



2.3 Protecting Your Workplace

A terror attack at a poorly protected workplace could result in injuries and loss of lives of employees. A cyber attack could result in sabotaged IT systems, disrupted supply networks and business operations. Hotels can also incur costs from rebuilding, insurance pay-outs, lowered profits, the loss of investor confidence and dropping employee morale.

These impacts may be prevented or minimised by enhancing workplace security in the following ways:



Deter

Implement measures that make potential attackers see your hotel as too difficult, risky or dangerous to strike.



Delay

Put physical and system barriers to slow the progress of an attack on your hotel, allowing security and IT teams to respond and mitigate harm.



Detect

Find and address signs of terrorism or cyber crime as early as possible, lowering the harm or threat they pose.



Deny

Safeguard employees and guests by ensuring that only authorised persons can access important information or areas.

Challenges Hotels May Face

- Balancing guests' convenience and comfort against added security procedures
- Costs of installing physical deterrents or implementing new technology
- Retaining the character of old buildings while retrofitting them to be more secure
- Finding appropriate individuals to implement and monitor security upgrades

You may use the following guidelines to identify actions that suit your hotel's security needs and risk levels.

Policies and Procedures

Though short-term costs may be incurred, planning your hotel's crisis response is critical to safeguarding the business' long-term interests. Reviewing your plans regularly also ensures that any new gaps in security can be patched before they are exploited. By improving your hotel's ability to spot unusual activity, you can better deny terrorists and cyber criminals access to your premises, systems and data.



Senior Management

Manpower Deployment

- ☐ Enrol employees in the **Corporate First Responder (CFR) Scheme**, which gives them a Cordon Pass to enter restricted sites and assist with recovery efforts if an attack occurs (see page 70)
- ☐ Standby a pool of professional counsellors who can be contacted to provide psychological first aid for guests and employees

Safeguarding Your Business

- ☐ Formulate business continuity plans on how your hotel would recover from a terror or cyber attack
- ☐ After any incidents, review the activity log to identify loopholes and areas for improvement, and then revise your existing plans accordingly
- ☐ Register for the **Workplace Safety and Health Council's bizSAFE programme** to improve your hotel's safety, health and security capabilities



Scan QR code to sign up for a complimentary bizSAFE Level 1 workshop



Security Personnel

Safeguarding Your Business

- ☐ Prepare copies of up-to-date contingency plans, ground layout, floor plans, and locations of exit points, EHA, CCTV, AED, fire hoses and means of communication (e.g. walkie-talkies), and provide these to senior management or authorities in the event of a crisis
- ☐ Keep these documents and information securely, yet readily accessible to authorised personnel only

General Procedures

- ☐ Create and maintain an incident activity log, with an employee assigned to update it as events occur
- ☐ Develop a procedure to control how off-site personnel may gain access to restricted areas, both during regular operations and during a crisis



Non-Security Operations

General Procedures

- ☐ When handling lost room keys, verify the identity of any individuals requesting new or extra keys
- ☐ During peacetime, create open channels of communication with hotel administration and senior management to ensure everyone is updated promptly
- ☐ During a crisis, help to ensure all guests are accounted for and kept aware of any developments that may occur



Hotel Administration

Safeguarding Your Business

- ☐ Create templates for public communications during a crisis to prevent miscommunication
- ☐ Work with Senior Management to develop plans to stabilise the situation in the immediate aftermath of crises
- ☐ Develop post-crisis marketing and publicity plans to aid in business and revenue recovery

General Procedures

- ☐ When employees have resigned or are terminated, review their access rights (e.g. employee passes, biometric information, keys and passcodes) to prevent them from obtaining sensitive information or entering secure areas
- ☐ Create procedures to handle loss of any form of security pass (including both physical keys and digital passwords)




Day-to-Day Operations

Ultimately, the people who work in your hotel are the ones who will ensure it is safe and secure. It is important that every employee – from non-security operations to senior management – keeps a look out for suspicious activities or individuals on a daily basis. This is critical in detecting terrorist activity or signs of cyber terrorism before it escalates to a crisis.



Security Personnel

Manpower Deployment

- ☐ Station employees or security officers at restricted access areas and ensure they are able to identify persons and vehicles permitted to enter
 -  If manpower constraints do not allow you to station security officers, you could encourage all employees to look out for unfamiliar persons or utilise technology substitutes, such as CCTVs, to monitor for intrusions and cover more ground

General Procedures

- ☐ Look out for vehicles parked for a prolonged period of time, and question vehicle owners about their presence
- ☐ Enforce strict access control measures by only allowing those with employee badges and passes or authorisation letters (for third parties) to enter restricted or employee-only areas
- ☐ Conduct regular, but unannounced patrols and inspections at vulnerable areas, or engage a vulnerability or penetration testing service





Non-Security Operations

General Procedures

- ☐ Stay alert to possible signs of terrorist activities when performing tasks like accepting deliveries, cleaning and interacting closely with guests (see page 58)
- ☐ Maintain records on holders of all keys, and restrict access to master keys
- ☐ Check and confirm the identity of third-parties and guests by ensuring the legitimacy of documents they provide, particularly if they are requesting room keys or information
- ☐ Log down and promptly report any suspicious incidents to security personnel
- ☐ **Some types of people an attacker or criminal may impersonate:**



Auditors or
government
officials



Third-party
contractors or
event organisers



Maintenance
employees



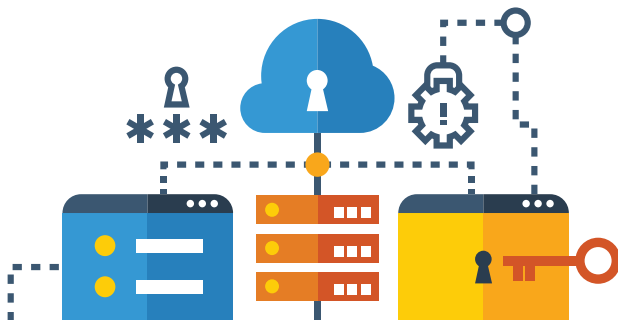
Delivery
drivers



Hotel Administration

General Procedures

- ☐ **Adopt the measures from Cyber Security Agency of Singapore (CSA)'s Be Safe Online Handbook (see page 66)**
 - Know what your cyber assets are
 - Allow only authorised software to work
 - Patch and update software in a timely manner
 - Be selective when granting admin account privileges
 - Detect breaches promptly
 - Control access via multi-factor authentication
 - Encrypt your critical information assets



Physical Infrastructure and Security Systems

Upgrading physical and security systems may have high upfront costs. However, these play a big part in deterring would-be attackers, delaying their attacks or denying their efforts to harm your hotel or guests.



Senior Management

- ☐ Work with Security and IT Personnel (for cyber security) to evaluate whether the current security expenses matches your hotel's needs and priorities



Security Personnel

Emergency Evacuations

- ☐ Establish lockdown procedures in preparation for an emergency lockdown
- ☐ Display emergency exit maps and important contacts in all guest rooms
- ☐ Ensure that evacuation plans can accommodate guests or employees with special needs
- ☐ Ensure all public, communal, and external spaces are clean and well lit, and keep the evacuation pathway clear of obstructions

Emergency Sites and Assembly Areas (AAs)

- ☐ **For non-terror incidents**
 - Identify at least two alternative AAs
 - Display clear directions to these areas
- ☐ **During terror incidents**
 - As AAs are vulnerable to secondary attacks, building occupants should not assemble or be ushered to them
 - You may account for employee safety virtually via online platforms or mobile messaging applications
- ☐ The **SGSecure Contingency Planning Checklist for Building Owners** contains additional resources such as guidelines to prepare the lockdown decision matrix for your hotel's contingency plan, and help for building owners to plan for contingencies such as terror attacks



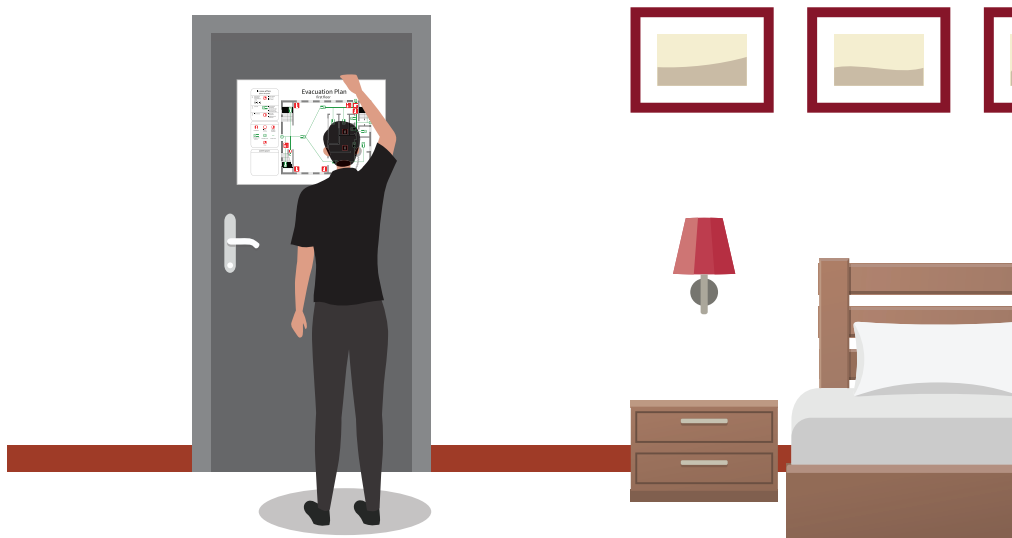
Scan the QR code
to download
the checklist

Emergency Storage/Shelters

- ☐ Allocate a readily accessible area for storage of emergency equipment and supplies
- ☐ Regularly inspect and replace faulty items, and ensure that the area is well-protected
- ☐ Designate shelter-in-place locations to protect guests and employees from external attacks

Exterior Areas

- ☐ Review security measures based on **Guidelines for Enhancing Building Security in Singapore (GEBSS)** (see page 66)
- ☐ Evaluate the ease of intrusion at the hotel perimeters and install perimeter barriers if needed
- ☐ Install barriers to keep vehicles a safe distance away from the hotel entrance and gathering areas
- ☐ Employ a speed control system to control approaching vehicles at the hotel entrance and other vulnerable areas of the proper
- ☐ Define the hotel perimeter and identify all possible exits and entrances
- ☐ Display signage to identify access points for guests, vehicles, and pedestrians
- ☐ Ensure that unused access points are sealed off or locked, and monitored for intrusion



Interior Areas

- ☐ Install panic buttons at vulnerable areas in the hotel
- ☐ Employ anti-shatter film, glazing protection or laminated glass to minimise injuries caused by flying glass pieces
- ☐ Install a Public Address (PA) system to aid in the mass dissemination of information and announcements during an emergency
- ☐ Adopt layered security by designing layered access points to critical areas
- ☐ Install access control devices at restricted areas, and maintain records of all access
- ☐ Use video surveillance where appropriate, and review footage of suspicious activities

Systems to Install

- ☐ Install intrusion detectors, motion detectors, fire and smoke alarms where appropriate
- ☐ Have a procedure in place for reacting to triggered alarms or detectors and exercise it regularly



Non-Security Operations

Interior Areas

- ☐ Conduct regular checks on all locks and access control devices to ensure they are functioning as expected
- ☐ If non-electronic keys are used, the serial number should be recorded in a log when guests check in or out of the hotel
- ☐ In the event of missing keys, replace your locks promptly





Illustrated Summary: Protecting Your Workplace

Security Personnel

- Ensure all employees are familiar with ERPs* and evacuation plans, and instruct them to avoid Assembly Areas during terror incidents
- Establish lockdown procedures and secure emergency storage or shelters
- Create guidelines to act on the presence of suspicious vehicles, people or items
- Review security measures based on **Guidelines for Enhancing Building Security in Singapore (GEBSS)** (see page 66)



Non-Security Operations

- Apply procedures to verify guests' identities if keys are lost
- Stay alert to possible signs of terror related activity
- During a crisis, help to ensure all guests are accounted for and kept aware of any developments that may occur





Senior Management

- Create business continuity and communications plans for terror and cyber attacks
- Regularly evaluate and upgrade security measures in exterior and interior areas
- Enrol employees in **Corporate First Responder (CFR) Scheme**



Hotel Administration

- Adopt the measures in **CSA's Be Safe Online Handbook**
- Monitor employee access rights and promptly remove those of resigned or terminated employees
- Work with Senior Management to develop plans to stabilise the situation in the immediate aftermath of crises
- Develop post-crisis marketing and publicity plans to aid in business and revenue recovery

2.4 Partnering Your Community

Terror attacks aim to destroy the trust that binds us together, driving colleagues, stakeholders, organisations and communities apart, reducing our ability to function as a society. Every hotel relies on a community to support on-going operations, so it is essential to form and maintain strong bonds by strengthening internal and external communication channels. By improving the coordination and flow of information, people may respond more quickly and decisively during a crisis, minimising unrest and disorder.

Engaging External Stakeholders

Suppliers



Non-Security Operations

- ☐ Identify alternative suppliers for food and beverages and amenities and ensure that you have channels of communication with them

Guests & General Public



Senior Management

- ☐ Develop written mutual-aid agreements with neighbouring hotels to provide affected guests with accommodation after a crisis
- ☐ Develop an information-sharing community to alert one another on incidents or detected threats so everyone can watch out for similar attacks



Hotel Administration

General Communications

- Alert employees and stakeholders on where to go for accurate and up-to-date information during and after crises
- Work with non-security operations to create, maintain and regularly update a contacts list of contractors, suppliers and business partners who can support business operations during a crisis

Emergency Communications

- Create and maintain an authoritative source of hotel information and provide constant updates on the crisis situation through your hotel's official social media channels and website
- Appoint a spokesperson to manage media relations effectively, and consider supporting them by registering them for crisis communications courses
- Engage the telecommunication providers in Singapore to develop restoration procedures in the event of a disruption to communication services

Third-Party Security Experts



Security Personnel

- Establish and maintain your own channels of communications to share information with both the authorities and fellow security leaders
- Join the **Safety and Security Watch Group (SSWG)** within your neighbourhood, so that you can:
 - Network with neighbouring buildings and the police to assess local threats
 - Pool knowledge and resources, and learn about safety and security best practices
 - Share tips with other hotels on how to strengthen building infrastructure against potential terror attacks

Engaging Your Employees



Senior Management

- ☐ Work with Security Personnel to test, refine and improve security plans
- ☐ Organise engagement activities to promote a vibrant and united company culture (e.g. small-group seminars or workshops on hospitality trends, virtual group-bonding activities)
- ☐ Implement grievance handling procedures to allow aggrieved workers to seek help



Security Personnel

Emergency Communications

- ☐ Set up a **Crisis Command Centre** to control, monitor and coordinate your hotel's response to a crisis
- ☐ Set up a **Crisis Response Team (CRT)** with people from different departments
 - Should you designate the CERT as the CRT, provide briefing and training on their expanded roles
 - You may use the template on the SGSecure@Workplaces website to do so



Scan QR code to
visit the SGSecure@
Workplaces website



Non-Security Operations

- ☐ Befriend and support one another, and proactively join and organise ground-up initiatives like meals after work to build team spirit and cohesion
- ☐ Consider having a department-based platform to directly communicate with, or raise security concerns to higher management



Hotel Administration

General Communications

- Where permissible, organise face to face or virtual team-building activities to encourage and motivate employees (e.g. themed online meetings where employees can participate actively)



If large-scale activities like Dinner and Dance events or employee retreats disrupt your daily operations, consider implementing regular, small-scale initiatives (e.g. suppers after work, birthday celebrations, etc.)

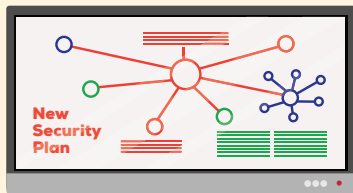
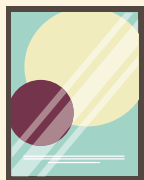
- Communicate regularly with your employees through informal face-to-face engagements or other feedback channels
- Create opportunities where employees from different departments can interact with one another, share updates on terror, cyber trends and news and discuss security issues which your hotel faces

Emergency Communications

- To pre-empt questions and concerns that may arise in response to the crisis, try to draft FAQs and replies in advance to ensure that you can give a timely response during a crisis (e.g. employees may ask if they should report to work, and hotel guests may ask for refunds for booking cancellations)



Illustrated Summary: Partnering Your Community



Security Personnel

- Work with senior management to test, refine and improve security plans
- Join the **SSWG*** to network with neighbouring buildings, pool resources and learn about safety and security best practices
- Set up a **Crisis Command Centre with a dedicated CRT#**



Non-Security Operations

- Create and participate in activities to befriend and support one another
- Get to know employees in other job areas like security or administration
- Identify alternative suppliers for the hotel's F&B and amenity needs
- Consider having a department based platform to directly communicate with, or raise security concerns to higher management





Hotel Administration

- Prepare a list of key contacts (e.g. contractors, suppliers and business partners) to support post-crisis operations
- Establish procedures to restore communications in crises for both employees and hotel guests
- Establish an official online presence to disseminate information and correct rumours
- Communicate regularly with employees and act promptly on feedback

Senior Management

- Work with neighbouring hotels to room guests affected by crises
- Promote a vibrant, united company culture
- Implement grievance handling procedures



3.1 Innovative Practices from Local Hotels

The resources and recommendations in this guide are intended to be guidelines that you can pull from as you create your own hotel's security policy. There is no single best practice or routine to follow – instead, hotels are advised to adapt from the guide to suit their circumstances.

The hotels below have found creative ways to balance between enhancing security, satisfying guests' needs, and maintaining a hospitable image.

How a midscale hotel bordering the city hides security features in plain sight

Hotel Statistics



202
Rooms

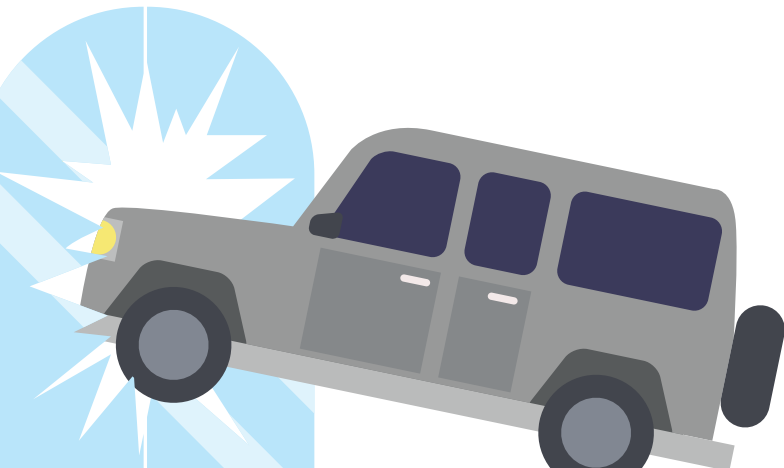


120
Full-time Employees



What They Practise

Crime Prevention through Environmental Design (CPTED)





Their Challenges

- ☐ A clear glass exterior allowed people to look into the hotel at night and observe employee movements, security patrols, locations of VIPs and guests, and even security passcodes
- ☐ Vehicles could potentially ram through the building's exterior from the driveway, but installing large barriers to prevent this would have affected the hotel's overall aesthetics



Their Measures

- ☐ **Installing wind-down curtains:** The curtains can be lowered at night or during events, preventing external parties from viewing and observing events inside
- ☐ **Hiding bollards inside large flowerpots along the driveway:** This provides a concealed physical barrier that can slow down speeding vehicles, even as the hotel is looking into other creative ways to further enhance building security with the installation of ramps or humps



How a centrally located midscale hotel enhances security with technology

Hotel Statistics



420
Rooms



240
Full-time
Employees

20
Part-time
Employees



What They Practise

Utilising technology to enhance security



Their Challenges

- ☐ In the event of an emergency, the hotel will need to alert guests, mobilise security personnel, and get employees to report in safely all at once, which would require a large effort to coordinate
- ☐ Gathering people at assembly areas could create an opportunity for terrorists to launch secondary attacks, resulting in more damage and possible loss of lives
- ☐ The hotel wanted its security personnel to be able to cover more ground and respond faster during emergencies, but without incurring significant manpower costs

Their Measures



- ☐ **Equipping every guest room with a mobile device that provides free international calls:** In the event of a terror attack, hotel management can send out mass notifications to guests on ground areas to avoid
- ☐ **Providing security personnel with Segway personal transportation devices:** Gives security personnel greater ground coverage and higher efficiency compared to doing floor patrols on foot
- ☐ **Connecting critical CRT members' phones to security personnel's walkie-talkies:** Allows all parties to stay connected even when they are not physically present
- ☐ **Developing an in-house mobile app for employees:** Enables employees to remotely report their safety statuses during a crisis, thereby eliminating the need for an assembly area



How a centrally located luxury hotel prepares its employees

Hotel Statistics



792
Rooms



980
Full-time
Employees

1000+
Part-time
Employees



What They Practise

Providing employees with anti-terror tools and knowledge



Their Challenges

- ☐ It was easy for employees with a regular routine to simply go through the motions of security preparedness, without internalising the things they have learnt
- ☐ Translating the theory of what employees learnt to real-life situations could be difficult as employees tend to panic and forget important protocols during crises
- ☐ Pre-established procedures may also have loopholes that need to be identified, to ensure that crisis management runs smoothly in the event of a real attack



Their Measures



- **Creating an emergency hotline:** Employees and guests can use the hotline to report any suspicious activities they spot, and each employee also has a card with the hotline printed on, together with the slogan 'See Something, Say Something'
- **Conducting regular simulation drills:**
 - Employees are tested on their reactions during the drills, before security personnel identify gaps in how situations are handled
 - Learning points are then consolidated and shared with employees involved so that they know the right courses of action to adopt in future
- The simulations include situations such as:
 - An employee pretending to be drowning in the pool
 - A housekeeping employee pretending to be locked inside a room (using dry ice to create a scenario of smoke from fire coming through the gap in the door)
 - Leaving an unattended, suspicious bag at different areas of the hotel



3.2 Responding in the Event of a Terror or Cyber Attack

Terror Attacks

In the event of a terror attack, knowing how to respond swiftly and decisively amidst the chaos can make the difference between life and death.



Response measures that anyone can undertake in the event of a terror attack:

- ☐ If at the site of an attack, Run, Hide, and Tell immediately
- ☐ Perform Improvised First Aid Skills (IFAS), or Press, Tie and Tell, to stop the bleeding of casualties
- ☐ Cooperate with appointed hotel employees and security personnel as they evacuate employees and hotel guests
- ☐ Instruct employees and hotel guests to run as far as possible from the site of attack
- ☐ Find remote ways to check on the safety of employees (e.g. update on safety status via group chats)
- ☐ Provide the police and authorities with any relevant information to facilitate investigations
- ☐ Avoid circulating internal information, photos, or videos via social media, as doing so may create unnecessary panic and misinformation



Security personnel, in particular, play a crucial role in coordinating the response protocols with other departments, and ensuring everyone is familiar with their roles in a crisis. You may refer to pages 12 and 66 for online resources to share with employees.



Security Personnel

- ☐ Ensure that the Fire Command Centre is secured and readily accessible by required parties
- ☐ Activate your hotel's ERP
- ☐ Utilise pre-existing communications channels such as alarms or the PA system to alert employees and hotel guests
- ☐ Hand over copies of the hotel's key information to authorities if needed (see page 24)
- ☐ Activate building lockdown procedures to protect occupants who are in close proximity to an immediate threat
- ☐ Consider conducting a security sweep of assembly areas to ensure that there are no risks of secondary attacks present
- ☐ Alert neighbouring buildings of the attack, if possible



Cyber Attacks

Your hotel may use digital and cloud services to facilitate operations, such as online booking systems, loyalty programmes, cashless POS systems and more. You can prevent these from being exploited through implementing strong cyber security measures and establishing a response plan to handle cyber attacks.



Cyber Attack Facts

□ Overview of the Cyber Threat Landscape

- Cybercrime continues to be on the rise in Singapore, with 9,430 cases reported in 2019 (up 51.7% from the 6,215 cases reported in 2018)
- 47,500 phishing URLs with a Singapore-link were detected in 2019
- From 2018 to 2019, organisations in Singapore that were hit by cyber attacks came from all industries, including hotels



Scan QR code to
read more

What Form Can Cyber Attacks Take?

The majority of cyber threats in Singapore took the following forms:



Ransomware

A type of malware that cuts off access to the victim's files, systems or devices until a ransom is paid. Ransomware can spread through emails with malicious attachments or links, where unsuspecting users open these attachments or links.



Phishing

This refers to emails or messages that appear to come from a reputable source, such as banks. The goal of such emails is to obtain security credentials or personal data from users. For example, attackers could use spoofed email accounts to impersonate a hotel's CEO, business partner or known contact of the victim to request data from him or her.



Web application attacks

This is when attackers use methods like SQL injections or Cross-Site Scripting to gain access to applications such as cloud servers and business databases.

If a data breach happens, your IT departments or managers in charge of the area should act as soon as possible to alleviate damaging consequences and limit financial or data losses.



Hotel Administration

- Identify how the attack occurred
 - Payment systems and cloud-based storage of guests' data (e.g. from loyalty programmes) are common points of attack
- Determine the extent of the compromise
 - For businesses that own e-commerce platforms, the personally identifiable information and payment details of customers may be targeted
- Perform a security check on all affected systems
- Report the incident to the relevant authority or organisation
 - Lodge a police report
 - Report the cyber incident to the Singapore Computer Emergency Response Team (SingCERT)
 - Notify the Personal Data Protection Commission if there is a data breach



Scan QR code to fill in the SingCERT's Cyber Incident Reporting Form



Scan the QR code to see when and how you can report a breach

- Broadcast relevant information to affected customers, colleagues or tenants
 - Address their concerns about how the incident occurred and inform them of the measures that have been taken to resolve the issue and/or the steps taken to safeguard their data

4.1 Recovery Efforts of Hotels

Terror attacks may leave devastating consequences, damage infrastructure and create tensions between social groups. Emotional distress may grow amongst employees even if they were not direct victims of an attack. Including strategies to mitigate such negative effects in your recovery plan ensures that your hotel's operations can swiftly return to normalcy.

This section will explain how you can stay in touch with your stakeholders and suppliers during times of emergency. You will also learn how you can provide psychological support to employees and hotel guests.



Senior Management

Supporting Your Employees

- ☐ Arrange for Psychological First Aid and support for affected employees



Security Personnel

Enhancing Overall Security

- ☐ Activate pre-established business continuity plans
- ☐ Take note of gaps in existing contingency plans and adopt measures to enhance hotel security
- ☐ Download contingency planning and protective security advisories from SPF website (see page 70)
- ☐ Refer to authoritative sources of information, such as the SGSecure mobile app, or the hotel's social media channels and official website, for updates and information on possible security measures to implement





Non-Security Operations and Hotel Administration

Continuing Business Operations

- ☐ Activate pre-established business continuity plans, which can include measures such as hotel room and banquet room booking promotions to draw guests back
- ☐ Contact contractors or suppliers to assist in continued operations and infrastructure recovery
- ☐ Send out positive messages through influencers, public figures and the media to restore the image of Singapore as a tourist destination
- ☐ Consider targeting new market segments that may be more resilient to crises, or offering alternatives to traditional overnight stays (e.g. promoting your hotel to local guests, or offering work from hotel packages)
- ☐ Instead of downsizing, consider retraining employees to fill different roles for better service recovery after the crisis has passed



Hotel Administration

Supporting Your Employees

- ☐ Take a strong stance towards discrimination at the workplace, and ensure the Human Resources department addresses the cases promptly
- ☐ You may also disseminate circulars to promote unity and cohesion among employees
- ☐ Contact the Singapore Red Cross Society for Psychological First Aid courses (see page 69)
- ☐ Provide post-crisis support for affected employees and refer them to professionals, if necessary
 - Seek out counselling centres to support traumatised frontline employees who experienced the attack firsthand and may require professional counselling (see page 72)