# Fortifying Customer-Facing Businesses: The Defence in Depth Security Approach

*By Col Kanwal Kishore, SM (Retd)*

Terrorist threat looms large on 'soft targets,' customer facing enclosed spaces. It has become imperative to enhance security measures in closed 'customer-facing' venues such as theatres, malls, hospitals, movie halls, airports, or religious places. Though it's not possible to stop an armed intrusion without having fire power, however, measures can be taken to delay/deny entry to perpetrators.

As part of physical security for customer-facing businesses, "**Defence in Depth**" needs to be planned from design stage and implemented on ground with letter and spirit. Defence in Depth is a military term which simply means a multi-layered security approach designed to protect assets by implementing several layers of security measures.

Following measures can be adopted to safeguard property, people, and infrastructure.

1. **Perimeter Security**:
    a. **Physical Barriers**: Installing bollards, fences, walls, or boom barriers to prevent unauthorized access to the premises.
    b. **Access Control Points**: Controlled entry and exit points equipped with security personnel, surveillance cameras, and electronic access systems.
    c. **Vehicles Screening**: Gantry Systems, UVSS and EVTDs are critical for screening incoming vehicles for explosives or suspicious items.
2. **Building Security**:
    a. **Surveillance with Analytics**: Use analytics of CCTV cameras, sensors, and alarm systems for pre-warnings.
    b. **Equipment**: Robust use of XBS, DFMDs, HHMDs are essential for screening individuals and detecting concealed weapons or explosives.
    c. **Security Personnel**: Trained guards stationed at key points to monitor and respond to security threats.

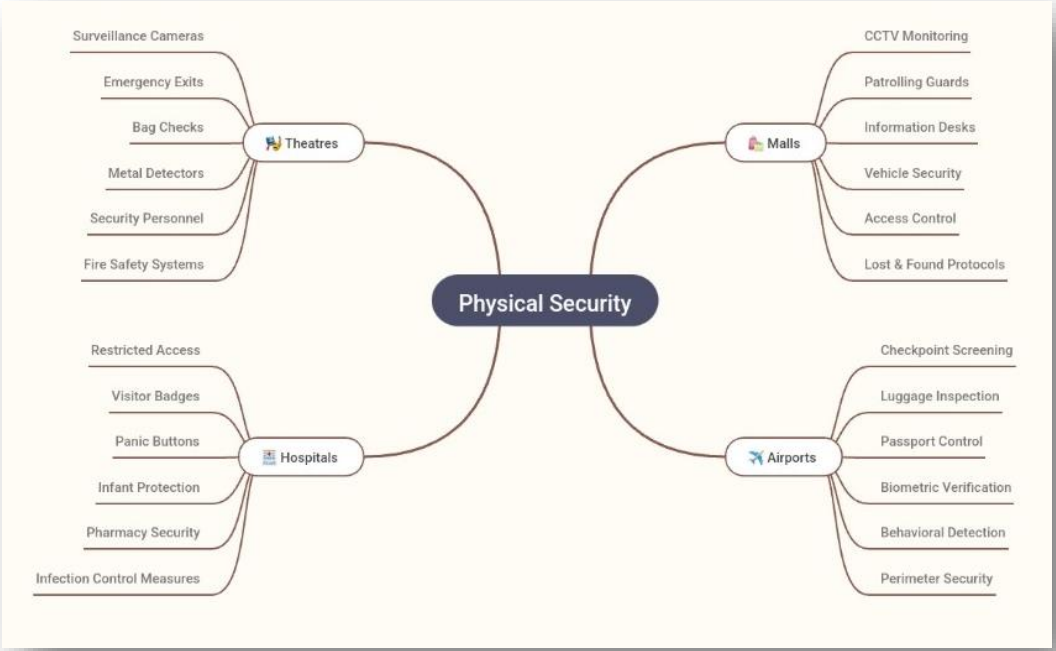
3. **Internal Security**:

   a. **Access Control**: Restricted access to sensitive areas within the business, using key cards, biometric systems, or security codes.

   b. **Visitor/Vendor Management**: Implementing a visitor check-in/check-out system to track and monitor visitors.

   c. **Background Verification:** BGV and credential verification processes are essential for ensuring that individuals accessing the venue, including employees and contractors, do not pose a security risk.

   d. **Security Training**: Regular training for employees to identify and respond to security threats effectively.




4. **Evacuation Plans**:

   a. **Emergency Exits**: Clearly marked and easily accessible emergency exits to evacuate people safely during emergencies.

   b. **Emergency Communication**: Systems in place to quickly communicate with employees and customers during emergencies.

5. **Incident Response**:

   a. **Security Protocols**: Establishing clear security protocols and procedures to follow in the event of a security breach or threat.

   b. **Collaboration with Law Enforcement**: Building a strong relationship with local law enforcement agencies to facilitate a rapid response to security incidents.

## 6. Importance of Security Operations Centre

A well-equipped and manned GSOC is indispensable for centralized surveillance, rapid threat assessment, and coordinated security response across customer-facing venues such as theatres, malls, hospitals, movie halls, or airports. It enables proactive monitoring, timely detection, and effective management of security threats, thereby enhancing the overall security posture and ensuring the safety and security of customers, employees, and assets. Implementing a robust GSOC is crucial in today's threat environment to mitigate risks, respond effectively to security incidents, and maintain a secure and resilient environment for conducting business and serving customers.

## 7. Intelligence and Vigilance


a. **Internal & External** - The significance of intelligence and vigilance plays a crucial role in corporate security, aiding in the early detection of potential threats and enabling teams to be well-prepared for likely incidents. This team can be segmented to address both internal and external issues effectively.

b. **Social media** - Leveraging social media effectively is essential for this team to gather relevant information and intelligence. The team serves as the *eyes and ears* of the organization, continuously monitoring the security landscape to identify emerging threats and vulnerabilities.

c. **Approach & Flow of Information** - Their proactive approach to gathering and analysing information allows the organization to stay one step ahead of potential risks, ensuring a more secure and resilient environment for conducting business. Moreover, the ability of this team to collaborate closely with other security functions, such as the GSOC or JOC, facilitates seamless information sharing and coordination, enhancing the overall effectiveness of the security operations.

This approach involves not only physical security measures but also operational and procedural measures to create a robust and resilient security posture against potential threats.