



Security Newsletter

JULY 2018 | ISSUE 11

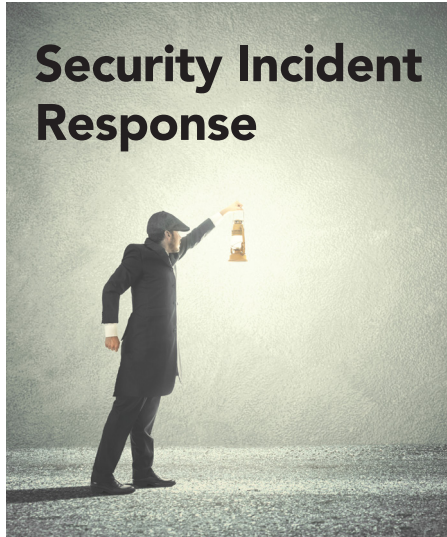
Physical Security Continued (III)

Whilst creating the overall physical security network, the following has been completed:

- Threat and risk assessments
- Separate independent perimeter has been established (or using the building itself as a perimeter),
- Secured internal spaces
- Locked doors and windows
- Secured confidential information
- Created staff, visitor and vehicle access controls
- Installed adequate security lighting
- Set-up electronic surveillance and recording systems, and
- Created a manned security force

All the necessary components are in place, now the challenge is how to effectively deploy the resources, supervise their operation and respond to any security incidents.

Security Incident Response



Knowing when an incident occurs Security officers are expected to effectively respond to a wide variety of incidents. So how do supervisors and management know when and where these are occurring?

Our information on incidents comes from a number of sources such as:

- An alarm is activated.
- When the incident is observed either on camera or by observation.
- Where the incident is reported either face-to-face, by telephone or other method.

How are incidents responded to?

Security personnel are usually tasked to respond to incidents by the security control room unless they actually see the incident themselves and have to take immediate action. Alternatively they may be advised by any member of staff or the public that an incident is occurring or has previously occurred which requires their response.

Security response depends on the type of incident which has occurred but all security responses should be covered by the organization's own Standard Operating Procedures (SOPs).

Standard Operating Procedures

The SOPs are the operational instructions available to an organization's security personnel detailing the actions they should take during specific incidents. They inform security officers of what to do in a particular incident, what actions they should take, who they should report to, what information is required etc. They also instruct security control room staff in their responsibilities to support and manage incident response.

SOPs should cover the various threats and risks which have been identified for a particular facility. They are many and varied but can include:

Some Standard Operating Procedures

- Incident response
- Fire
- Bomb Threat
- Evacuation
- Patrol procedures
- Pedestrian access
- Vehicle access
- Incident reporting
- Typhoon
- Door alarms
- Request assistance
- Person collapsed
- Key security
- Control room
- Supervisory procedures

Armed with the knowledge and procedures contained in their SOPs security officers can then respond efficiently and effectively to an incident.

However, to be fully effective the SOPs must cover all of the actions required during a particular incident, but most importantly the officers responding must be well trained and highly competent in their usage.



