bellrock

INNOVATIVE. TRANSPARENT. COMPLIANT.

Security Risk Management

Introduction to security risk management and advice during lockdown and re-entry.

www.bellrockgroup.co.uk

Security Risk Management

Employers have a general duty under Section 2 of the Health & Safety at Work Act 1974 to ensure, so far as 'reasonably practicable', the health, safety and welfare of their employees. Under section 4 of the Act, the party in control of a property also has a duty towards all people who are not employees, but use non-domestic premises.

The Health & Safety Executive states that an organisation must get help from a 'competent person' to enable it to meet the requirements of health and safety law. A competent person is someone who has sufficient training and experience or knowledge and other qualities that allow them to assist you properly. It therefore follows that building owners must appoint a competent person, familiar with security threats, vulnerabilities and security countermeasures to manage security risk.

The law does not expect building owners to eliminate all risk, but it does require the protection of people insofar as 'reasonably practicable'. Building owners are also required to set up emergency procedures, provide information to employees and work together with employers sharing the same workplace. The term 'workplace' also includes common parts of shared buildings, private roads, etc.

In extreme circumstances, organisations can be prosecuted where gross failure in the way activities were managed, or organised result in death. Courts can impose unlimited fines and a publicity order requiring organisations to publicise details of its conviction and fine. In terms of reputation it is therefore critical for building owners / managers to appropriately assess and manage security-specific risks.

There are various security industry guidelines, or standards for managing security. In the UK, the industry widely has regard to an ASIS General Security Risk Assessment Guideline and guidelines published by the Centre for the Protection of National Infrastructure (CPNI). CPNI is the government authority for protective security advice to the UK national infrastructure, accountable to the Director General of MI5.

In accordance with CPNI guidelines, security planning must not evolve in an arbitrary or ad-hoc manner or develop solely from previous mistakes and errors. No single security response, or level of investment will provide 'total' protection. Nor is it practical for organisations to invest in every solution available. However, a considered and up-to-date security plan, appropriate to the organisations and in proportion to the risks they face can help to protect against the worst possible consequences.

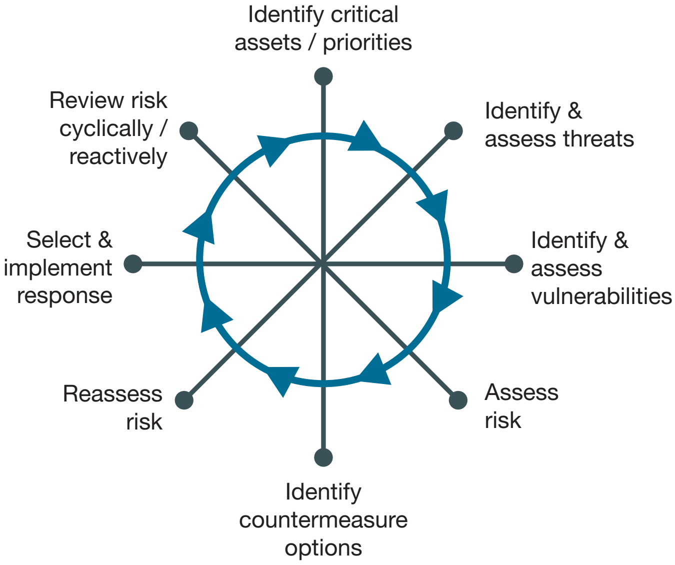
To be effective, a security plan must be fully integrated with everyday operations and needs to be 'multi-layered', where each measure is reinforced by the next. Security measures can be resource intensive, costly and if not carefully managed, disrupt routines and alienate members of staff. This is why careful consideration and planning is required when choosing the right response and why specialist advice should be sought.

As a general guide, the following principles should be central to any decisions:

- It is not possible to protect everything so prioritise the areas to protect
- Measures should be proportionate to the threat
- Do not let the cost exceed the value of the asset being protected
- Security is more cost effective when incorporated into forward planning

An effective physical protection system must be based on a site-specific, security risk assessment, which should be carried out cyclically and in any event reactively.

A security risk assessment will determine; critical assets (what needs protecting / prioritising), security threats (what you are protecting against, further to intelligence gathering / analysis) and security vulnerabilities (weaknesses identified, further to survey of policies, plans, procedures, equipment and personnel). The typical security risk management process is set out below:


Identify critical assets / priorities
Identify & assess threats
Identify & assess vulnerabilities
Assess risk
Identify countermeasure options
Reassess risk
Select & implement response
Review risk cyclically / reactively

Security Risk Management

Further to carrying out a security risk assessment, it is possible to identify proportionate and cost-effective countermeasure options, having regard to the cost of potential loss. Physical protections is generally specified having regard to key security principles below, 3DR:

- **Deter**: This principle is often undervalued, although it is typically the lowest cost solution. Deterrence can be achieved through visible measures such as; signage, CCTV, lighting, or manned guarding.
- **Detect**: It is imperative to ensure that a potential adversary can be detected at an early stage, ideally externally (prior to breach) and notification measures are in place to enable response. CCTV and lighting are typically the key measures, particularly given advances in CCTV analytics. The two must however be properly integrated, to ensure compatibility and avoid conflict. Other measures include motion detection intruder alarms (internal / external).
- **Delay**: The typically physical security measures should protect the perimeter, all points of external access, all internal routes to upper / lower floors (stairwells / lifts) and any critical assets. It is important to consider all aspects of the barriers, including structures, locks, hinges, etc. Physical security is typically specified in accordance with the principle of 'Defence in Depth', which adopts a layered approach.
- **Respond**: The physical protection system must be set up to enable early detection and appropriate response. Response can range between; Public Address (PA) system, static guard response, remote response, or Police (depending on verification). Where remote response is adopted, appropriate physical security measures should clearly ensure early detection and delay, to avoid a significant loss event.

There are various ways to mitigate risk, including the 4 T's, which are set out below:

- **Tolerate**: To tolerate the risk, the probability and impact of the event may not justify the potential countermeasures.
- **Terminate**: It may be possible to terminate trading activities, such as arranging working from home, if that mitigates the risk and enables lockdown.
- **Transfer**: Security risk may to some degree be mitigated by insurance. The security risk assessment will consider the probability and impact of a loss event and therefore what should be covered under the insurance policy. For high profile buildings, it is now general practice to include cover for damage caused by riots / civil unrest.
- **Treat**: There are various ways to treat risk, including the following controls:
  - Preventative controls (e.g. physical protection equipment)

- Corrective controls (e.g. business continuity, or emergency response procedures)
- Directive controls (e.g. ensuring training and awareness of staff)
- Detective controls (e.g. post incident, asset register checks)

Security workforce during lockdown

On 26 March 2020, the SIA confirmed; 'Roles essential to supporting law and order, with the potential to reduce demand on policing, also meet the critical worker definition. This would include, amongst other areas, the guarding of empty or closed commercial, retail or office premises; the monitoring of similar through CCTV or other remote means; and the provision of alarm response centres including mobile units' and '…assess whether you can deliver more services remotely e.g. through CCTV. If a physical presence is required, then you should seek to minimise the number of staff deployed to the lowest safe level and ensure social distancing is applied'.

Therefore, it remains possible to secure sites by whatever means are considered necessary, including manned guarding. However, there is a requirement to consider whether security functions can be carried out remotely. At most sites, the level of resource during lockdown will simply be equivalent to typical out of hours, or weekend guarding. This often reflects the minimum resource levels.

During lockdown, the key is to regularly test the physical protection system to ensure it is effective, identifying any failures at an early stage and having measures in place to resolve them. Guarding can be employed, if a site is considered vulnerable.

Lockdown (partial / full) considerations

I have set out some key steps below, to assist building owners / managers, in managing the security risks during the period of reduced occupancy, or complete lockdown.

Security risk management

- Carry out a security risk assessment, to consider any changes to security threats, vulnerabilities and as such, necessary countermeasures.
- Consider suspending access rights for all but critical staff, depending on stakeholder approvals, or furloughed staff, having regard to insider threats.

Assignment instructions

- Review the site-specific assignment instructions, which should include partial / dynamic / complete lockdown procedures.
- Consider whether these procedures apply to the occupied status of the building.

Security Risk Management

Communications / IT

- Ensure the site IT network / telephone communications are maintained and reliable, to ensure monitoring of physical protection equipment.
- Ensure all key stakeholder contact details are up to date and ensure regular contact, to provide assurance and instructions regarding access / re-entry.
- Consult occupiers to determine re-occupation plans / volumes.

Deter

- Ensure there are appropriate deterrence measures in place, primarily signage, CCTV and lighting.
- Good housekeeping is essential to remove any potential reward.

Detect

- Consult the maintenance provider, to confirm whether remote monitoring of the physical protection system can be established and implement response procedures.
- Alternatively, ensure alarm, notifications and response procedures are appropriate and reliable.

Delay

- Ensure the physical protection system is proportionate to the occupancy levels.
- The number of external points of access should be limited and all other doors should be physically locked down, or secured and alarmed (where required for fire escape).
- Review access control permitted areas and fail open procedures.

Respond

- Subject to the status of occupancy and security risk, it may be appropriate to install a PA solution.
- Consult your security provider to determine a response procedure / commitment and availability of essential static guards, which are considered 'key workers'.
- It may be necessary to review Lone Worker procedures. Alternatively, consider outsourcing guard patrols at random, via a local service provider.

Systems

- Regularly assess system performance, including day / night CCTV, lighting levels, systems alerts (motion detection, access control, door management, etc), to ensure failures are identified at the earliest possible opportunity.
- Consider Uninterrupted Power Supplies for CCTV installations (access control controllers are typically supported).
- Carry out random surveys and testing. All access and lockup must be recorded and validated.

Maintenance

- Consult your maintenance provider to ensure essential maintenance activities will continue and confirm response procedures.
- Consider how maintenance activities will be coordinated during lockdown.

Insurance

- Ensure appropriate insurance is maintained and relevant to assessed security risks.

Compliance

- Review the full extent of the security team responsibilities and consider whether all statutory requirements are properly managed (H&S, fire, GDPR, etc).
- Ensure that all guard SIA licensing is kept up to date.

Re-entry considerations

Procedures

- Establish procedures for re-entry and communicate with all stakeholders. These are likely to be aligned with heightened threat level response procedures, set out within the site assignment instructions.
- Ensure all occupiers are aware of procedures and consult them regarding phased working hours, to reduce peak flow.
- Define thresholds for scalable increases in service delivery.

Full site patrol

- Carry a full patrol of the site, to identify suspicious items in advance of re-occupation. Ensure findings are recorded and reported to senior management.

Risk management

- Consult stakeholders to ascertain whether there is any change to the threat to each business.
- Consider setting up a local business forum and establish contact with the local Police, for local regular updates.

Systems

- Ensure all physical protection systems are operational and tested.

Signage

- Implement clear and concise directional and procedural signage.

Security Risk Management

Guarding

- Review assignment instructions to determine essential, scalable resource requirements, subject to stakeholder consultation regarding foot fall.
- Consult the security service provider to determine a procedure for reinstating services.
- Consider remote monitoring during reduced guard numbers, to enable focus ‘on the ground’.

Points of entry

- Consider minimising points of access, proportionate to security resource oversight.
- Consider thermal imaging CCTV, validation and procedures in consultation with stakeholders.

Stakeholders

- Consider procedures for separately managing occupier, visitor, delivery, collection screening / access.

Access control

- Reinstate authorised personnel access control.
- Consider a concierge guard, to deter and check ID.

Social distancing

- Consider protection measures for security staff, including stand-off distance and sanitiser.
- Reduce touch points, such as open doors, use of stairwells and restricted lift access (designated upper floors, number of people).
- Consider replacing ‘push to exit’ access control buttons with proximity contactless solutions (power source may be required).
- Consider one-way foot flow.

Ongoing review

- Continue to monitor and analyse access numbers and general performance.
- Provide regular status updates for stakeholders, until a return to ‘normal’.

Key Points

Carry out a security risk assessment, to ensure an effective physical protection system (deter, detect, delay, respond).

Review assignment instructions (plans / procedures) and consider scalable resource thresholds.

Review permitted access control, in consultation with stakeholders.

Consult stakeholders to determine re-occupation plans.

Consult security providers (guarding / maintenance), to determine response procedures and commitments.

Regularly assess systems (IT / physical security) performance.

Carry out a full patrol of site, to identify suspicious items in advance of re-occupation.

Consider social distancing and reducing / altering touch points.

Ensure ongoing statutory and insurance policy compliance

Keith Douglas | Service Charge Consultant / Security Consultant
CSC PGCertSM

keith.douglas@bellrockgroup.co.uk
+44 (0)08903 500 455

Keith is Bellrock's professional security consultant, carrying out security risk assessments at large commercial office and retail developments. He is able to assess critical assets, security threats and vulnerabilities further to survey and specify proportionate countermeasures (including; policies, plans, procedures, equipment and personnel) having regard to key security principles (deter, detect, delay, deny / respond), depth in defence and CPTED.

Bellrock Property & Facilities Management Ltd

Peat House
1 Waterloo Way
Leicester
LE1 6LP

e: enquiries@bellrockgroup.co.uk
t: 0116 464 0800

LinkedIn

www.bellrockgroup.co.uk