HARRIS
SECURITY MANAGEMENT

Security and Emergency Risk Management Solutions •
Security Risk & Vulnerability Assessments •
Integrated Security Systems Design •
Emergency Planning & Management •
Security Management & Systems Audits •

Phone: (02) 9560 9933
info@harris.com.au
www.harris.com.au

COVID-19, Security and the F-word

Will your security risk management support you during the next pandemic?

With the easing of COVID-19 restrictions many organisations are preparing to welcome back their personnel and to resume business activities.

Novel virus – novel business landscape. With a future even more uncertain than before COVID-19, managers need to re-focus on their security risk management to ensure that their changing organisations are supported and resilient in the security sense. Failure to do so may have serious consequences.

To be **pandemic security-ready** is a multi-contextual necessity. Commercial CBD properties, shopping centres, commercial tenancies, university faculties, health facilities, schools, government agencies, distribution centres, places of worship and NGOs are examples that need to be pandemic security-ready. The consequences of security risk management failure need to be fully understood before the next pandemic.

One of Worksafe Australia's COVID-19 Workplace Safety Principles, states:

> "To keep our workplaces healthy and safe, businesses must, in consultation with workers, and their representatives, assess the way they work to identify, understand and quantify risks and to implement and review control measures to address those risks."

Clearly, this advice is in the health and safety context of COVID-19. However, from our security risk management mindset, this principle should be extended to security and related risks that have been impacted by COVID-19, thus broadening the context. After all, a workplace risk is a workplace risk. It's about governance and resilience.

It is pleasing that many employers and commercial property managers are thinking about resumption of on-site operations in the COVID-19 context and have developed plans and provided advice. However, security and related risks require greater attention than what most of these plans and advisories provide.

Based on COVID-19 experiences and the expected changes to organisations, workplaces and marketplaces plus the energised drive for new thinking, new knowledge, new trajectories, new management and technical systems and perhaps new corporate cultures, the following are actions to focus your physical security capability and contribution for the next pandemic.

Some Assumptions:

- **Security plans and procedures** - Assume standing plans and procedures have lost currency especially relating to staged or large scale return-to-work activities, the evolving workplace or facility and associated security risks. The new business as usual (BAU) is not yet known. The need to stay agile may require a shift from security procedures to security guidelines in some circumstances.
- **Security resources** - Assume security resources may not have the capacity or alignment to support security objectives. For example, some organisations may identify that there is a need for an additional security officer or concierge at least for anticipated higher demand or surge periods for close oversight, such as managing lift lobbies with limits on people allowed into each lift.
- **Crisis management** - Assume your organisation will be re-evaluating its crisis management, especially in relation to pandemics. Ensure the crisis committee is an active player in the development of your organisation's security risk management.
- **Personnel returning to (traditional) workplace** - Assume personnel will have forgotten some essential security and emergency management knowledge.
- **Training updates** - Assume updates need to be provided to members of the facility's emergency command organization (ECO), of particular note floor wardens employed by tenants in commercial office properties, faculties within universities and similar arrangements in other complex locations.
- **Wardens** - Assume not all wardens will be returning to this role. This may be due to new working from home (WFH) arrangements, possible retirement of some wardens in higher health-risk categories concerned about the public health situation, perhaps a commercial tenant (that provided wardens for the ECO) has closed down due to economic conditions, or some other reason. If this is an issue, early consultation with in-house emergency management specialist or external consultant should be considered to ensure compliance and safety.
- **Staff thoughts and behaviour** - Assume returning personnel will not have security and emergency management central to their thoughts or behaviour (unless in a regulated workplace). Family concerns regarding COVID-19 may also be a factor. This is an example of a cultural issue when people in charge of security should talk with their HR specialists.
- **Criminal attraction** - Assume less than (old) normal number of occupants may attract criminality, including by trusted insiders. Examples may be offices (such as in CBD office buildings) not re-occupied or only partially occupied, or common areas (such as end-of-trip facilities).
- **Availability of security staff** - Assume security officers and security technicians will not be available during the next pandemic. Consider remote (off-site) operation of security and surveillance systems (situational awareness) and capability to remotely assess technical performance (e.g. each surveillance camera) and conduct remediation of these systems.

- **Updates to personnel** - Assume your personnel will be scattered and isolated during the next pandemic. They will need to be updated with accurate and timely information. They will expect it. Mass emergency notification systems can be used very successfully during a pandemic (or indeed all types of emergencies and critical incidents). Our prediction is that COVID-19 will increase interest in these systems.
- **WFH physical and cyber security** - Assume some personnel will be working from home as a common practice from now on. Consider physical and cyber security risks at home. Their home is their workplace, which has legal implications. As well, personnel working from home should be identified as 'lone workers'. This arrangement requires specific risk assessments, plans, procedures, guidelines and systems.
- **COVID-19 Mark-II or another pandemic** - Assume that this will occur during your employment at this facility or with this employer.

  NOTE: Assumptions to help conceptualise review frameworks can be beneficial. Some may be proven wrong when tested. However, there are other types of assumptions that should not be allowed, like 'our security is adequate for the next pandemic'.

Some Immediate Tasks:

1. **Issue** and communicate controlled advice and temporary amendments (to policies, procedures etc) relating to security issues in a timely manner. Security related communication may need to commence before personnel are physically on site.
2. **Audit** access control privileges and delete or change privileges based on the current access needs of individuals.
3. **Audit** all your security risk controls (for example, door alarms, emergency alarms and back-up power supply for security systems).
4. **Re-evaluate** PPEs based on recent experiences, in particular for facilities, security, concierge and ECO personnel. Specialist health and safety experts and proper risk assessments should guide your decision-making.
5. **Consider** on-site activities, especially those that will change. For example, businesses will be re-supplied, possibly using new suppliers. Social distancing will need to be maintained. This will possibly create changes to usage patterns, such as around reception areas, lift lobbies, loading docks and in-building cafes. It is anticipated that more people will request on-site and bicycle parking to avoid travelling on public transport. Consider the security risk implications and management options; for example, oversight by supervisors, controls and vetting, active video surveillance, temporary barriers and signage. Risk should be considered relevant to your context, for example unusual vehicle congestion including choke points, increased space and access requirements for garbage and re-cycling, increased on-site vehicle movements after-hours etc.
6. **Ensure** all personnel, especially new and temporary staff receive essential security and emergency management information, *now* not later. Security training needs to cover obligations, for example procedures to enter and egress the facility after-hours, reporting lost/stolen access control cards, reporting suspect behaviour etc.

7. **Provide** staff who have specific security responsibilities with refreshed and focussed awareness and compliance training.

8. **Ensure** the welfare situation of personnel including (contracted) security officers is understood and supported. Welfare of security officers is not done well by most security companies. The client may need to press the issue or fill the gap. It should be noted security officers around the world have been victims of COVID-19. For example, The UK Office of National Statistics (ONS) research identified that as at the 20 April 2020, men working as security guards had one of the highest rates of death from COVID-19, with 45.7 deaths per 100,000 (63 deaths). This must be a concern to security officers and their families.

Seek Facts and Assurance:

- **Assessments and reviews** - Conduct security (and emergency) risk assessments, vulnerability assessments and threat assessments. Differences between the last assessments and the current should be expected. Consider an independent review to validate and build upon reviews conducted in-house.
- **SOPs** - Audit and reassess security standard operating procedures (SOP) and security site (assignment) instructions to ensure these operational and governance instruments accurately and completely capture the new workplace, the new dynamics. Should there be no apparent reason to change SOPs and akin instruments, be confident that objectivity, expertise and lateral thinking are not missing.
- **Well-being -** Assess the well-being of security officers, even if they are contractors.
- **Emergency plan and emergency response procedures** - Review and reassess.
- **Research** – Research security risk management for WFH arrangements at other organisations. This should cover both physical and cyber security.

Some Update Actions:

- **Provide** updated security and crime prevention awareness training to occupants, as soon as possible and as frequently as required. Ensure genuine consultation and effective communication. A failure to identify and address security concerns held by occupants and other stakeholders may lead to unhealthy gossip and practices.
- **Update** your warden personnel list (and fill gaps).
- **Provide** refresher ECO emergency response training for ECO members.
- **Provide** emergency procedures training to occupants.
- **Update** security officer scenario training.

Strategic Focus:

- **Develop** a Security Plan **-** the garden variety security SOP alone (or in conjunction with the Emergency Plan) is not adequate for a pandemic, or indeed terrorism:
    - include responsibilities and actions of the security team and the facilities team, and others for example (depending on the organisation), crisis manager, communications manager, human resource manager, ICT manager, logistics manager and perhaps key suppliers and precinct neighbours. The Security Plan does many things, for example, it pre-approves authority,

    - resources, actions and lines of communication to meet elevated levels of threats.
    - provides opportunity to also properly consider those personnel who work from home, in regional areas or overseas.
    - security subject matter experts - should be considered to develop the Security Plan. If consultants are engaged, be aware that there may be licensing requirements in your jurisdiction.
    - provides evidence of governance, readiness, survivability and the hunger to thrive after the pandemic.

- **Evaluate** security contractors - Objectively evaluate your security contractor's performance and compliance. Some facilities suffered during COVID-19 due to their contractor's capability deficit.

    - Has your security contractor initiated conversations with you about how they will improve their readiness and sustainability next time, based on their COVID-19 experiences?
    - Articulate expectations - your expected governance and service requirements in specifications for security services and associated contracts. We often see during physical security vulnerability reviews and when providing expert witness reports for court, the inadequacies of these legal instruments.
    - Specifications – specifications for security service contracts require inclusion of requirements for a meaningful Business Continuity Plan (BCP) and Service Level Agreement (SLA) relevant to a pandemic (and terrorism).

Concluding Thoughts:

- As public movement increases and crowded places come back to life, expect terrorism related activities.
- Anticipate changes to physical design imperatives based on new hygiene principles and guidelines for facilities. This may impact security operations and may require re-configuration of your security and surveillance systems.
- 'Unprecedented' has been a term abundantly used to describe COVID-19. It is a term that should not be accepted as an excuse not to prepare for the next pandemic.
- Preparation to survive and thrive is central to leadership, governance, resilience, market advantage and reputation.
- Security risk management must be re-thought, re-aligned and re-invigorated.
- There will be another pandemic. Thus, the F-word - **Foreseeable!**

NOTE: The above discussion is of general nature only and intended to stimulate and focus conversation on security and related risk management. It lacks context. The above discussion is not comprehensive and does not provide expert legal comment or advice. The discussion does not provide professional advice. Seek expert analysis and advice relevant to your specific context from a trusted adviser.

Your comments are appreciated –
Geoff Harris, Principal Consultant, Harris Security Management
gharris@harris.com.au +61 419 462 798. www.harris.com.au