Are your site security risks as low as reasonably practicable (ALARP)?

In the UK, there are many chemical facilities that could be at risk from external physical and cybersecurity threats. Whilst many are covered by the Control of Major Accident Hazards (COMAH) 2015 regulations, only those considered to be Critical National Infrastructure (CNI) by the UK Government are specifically required to be protected against terrorist threats.

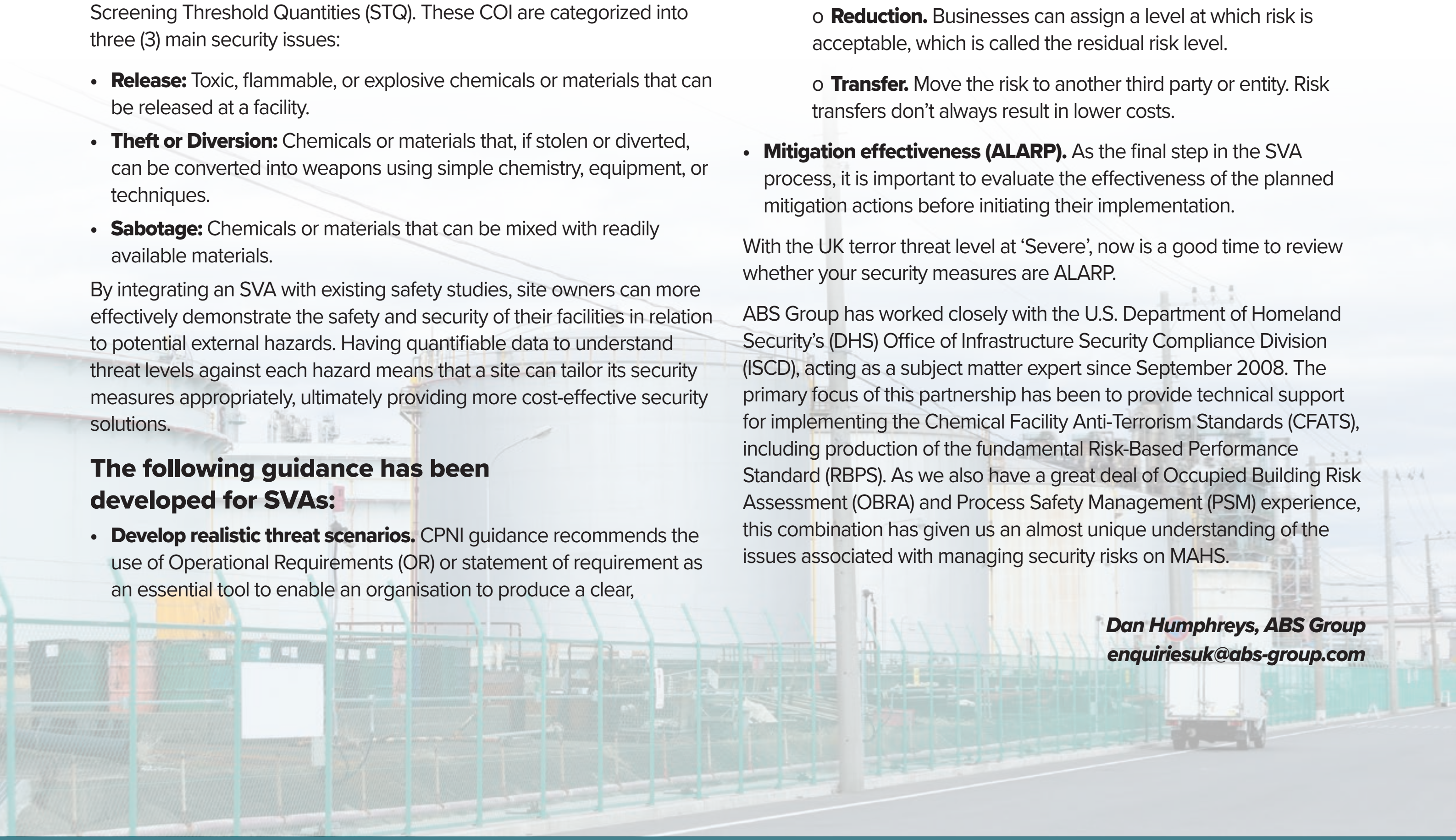
These sites are the focus of the Centre for the Protection of National Infrastructure (CPNI), which 'provides advice and assistance to those who have responsibility for protecting these crucial elements of the UK's national infrastructure from national security threats.' However, the UK terror threat level has remained 'Severe' since November 2021, begging the question: What do sites not designated CNI need to do to demonstrate an as low as reasonably practicable (ALARP) position for security risks?

From our global work with Major Accident Hazard Sites (MAHS), we have found that duty holders for hazardous facilities sometimes struggle to integrate Security Management Systems (SMS) with their requirements under Health and Safety legislation. Therefore, they can fail to develop a quantified ALARP position for security risk to the same level of detail as they would routinely provide within their regulatory safety justification.

A comprehensive Security Vulnerability Assessment (SVA) addresses chemical security by identifying whether you are a high-risk facility that possesses certain Chemicals of Interest (COI) above respective Screening Threshold Quantities (STQ). These COI are categorized into three (3) main security issues:

- **Release:** Toxic, flammable, or explosive chemicals or materials that can be released at a facility.
- **Theft or Diversion:** Chemicals or materials that, if stolen or diverted, can be converted into weapons using simple chemistry, equipment, or techniques.
- **Sabotage:** Chemicals or materials that can be mixed with readily available materials.

By integrating an SVA with existing safety studies, site owners can more effectively demonstrate the safety and security of their facilities in relation to potential external hazards. Having quantifiable data to understand threat levels against each hazard means that a site can tailor its security measures appropriately, ultimately providing more cost-effective security solutions.



The following guidance has been developed for SVAs:

- **Develop realistic threat scenarios.** CPNI guidance recommends the use of Operational Requirements (OR) or statement of requirement as an essential tool to enable an organisation to produce a clear, considered, and high-level statement of their security needs based on the risks they face. Mitigations to reduce the risk of theft are considerably different from those from an armed intruder.
- **Avoid unrealistic consequence assessments.** SVAs should be conducted in conjunction with the process conditions in the safety case submission to provide the most realistic results. When done in isolation, SVAs can predict consequences far larger than operationally possible.
- **Recognise shared security and process safety risk management barriers.** Unless specifically disabled by sabotage, barriers already instigated under PSM to mitigate the cause or effect of a loss of containment will still work during security-based scenarios. In conjunction with the use of process-based consequence modelling, the identification of existing barriers such as bunds, Emergency Shutdown Valves (ESV), gas detection or fire suppression could reduce the need for additional mitigations.
- **Apply risk-based mitigation strategies.** For realistic threat scenarios consider:

  o **Acceptance.** Understand the probability of it happening and accept the consequences that may occur. This is the best strategy when risk is small or unlikely to happen.

  o **Avoidance.** If the risk outweighs the benefit, stop performing that activity that causes the risk. Change the chemicals used or stop production of the product that makes the plant attractive to terrorists.

  o **Mitigation.** For risks that cannot be accepted or avoided, commit sufficient resources to control the risks identified through barriers to initiation or consequence.

  o **Reduction.** Businesses can assign a level at which risk is acceptable, which is called the residual risk level.

  o **Transfer.** Move the risk to another third party or entity. Risk transfers don't always result in lower costs.
- **Mitigation effectiveness (ALARP).** As the final step in the SVA process, it is important to evaluate the effectiveness of the planned mitigation actions before initiating their implementation.

With the UK terror threat level at 'Severe', now is a good time to review whether your security measures are ALARP.

ABS Group has worked closely with the U.S. Department of Homeland Security's (DHS) Office of Infrastructure Security Compliance Division (ISCD), acting as a subject matter expert since September 2008. The primary focus of this partnership has been to provide technical support for implementing the Chemical Facility Anti-Terrorism Standards (CFATS), including production of the fundamental Risk-Based Performance Standard (RBPS). As we also have a great deal of Occupied Building Risk Assessment (OBRA) and Process Safety Management (PSM) experience, this combination has given us an almost unique understanding of the issues associated with managing security risks on MAHS.

Dan Humphreys, ABS Group
enquiriesuk@abs-group.com