

Communications

An insider threat programme should integrate effectively with the organisation's overall communications' strategy. Care should be taken to implement insider threat-related security campaigns at the right time and to avoid confusion with other communications messages. If the messages are communicated appropriately, such channels can be very effective education and training mechanisms.

Communications relating to lessons learnt and case studies can both be impactful to help educate the workforce after an insider threat incident. They can also help employees understand the reasoning behind new security policies and procedures. Such stories should be balanced with positive case studies to help instil confidence in existing procedures.

Additionally, in the event that an insider threat incident occurs, it is important to have in place a communications response plan in the event that external partners or the media require updating.

Many of CPNI's campaign materials are linked below. They can be edited to include your organisation's branding if required. Each set of materials is accompanied by a programme plan, which should be carefully considered to ensure an organisation gets maximum impact from the campaign.

Existing Products

[All behaviour campaigns](#)

[It's OK to say](#)

[HoMER - Holistic Management of Employee Risk](#)

[Servator](#)

Security Minded Communications: For access, email enquiries@cpni.gov.uk

Deterrence Communications Toolkit: For access, email enquiries@cpni.gov.uk