National Protective Security Authority

NEWSLETTER – MAY 2023

NPSA Changes to Insider Risk Definitions

This document outlines changes being made by the UK's National Technical Authority (NTA) for personnel & people security specifically relating to *insider, insider risk, insider threat and insider event* definitions.

Background

Definitions enable us to have a common understanding of a word or subject; they allow us all to be on the same page and facilitate clear lines of communications. Having clear definitions of insider risk terminology is vital to support new and existing NPSA customers, who will have varying levels of knowledge in the subject area.

NPSA (formerly CPNI) has, until now, defined an insider as "*a person who exploits, or has the intention to exploit, their legitimate access to an organisation's assets for unauthorised purposes*". This definition was utilised for the purposes of the research underpinning the 2009 and 2013 Insider Data Collection Study. For the reasons outlined below, we felt it was the right time to refresh how we define our terms in relation to insider risk.

What is changing?

From May 2023 onwards NPSA will be utilising the following definitions through our various advice delivery and communications channels;

Insider	Any person who has, or previously had, authorised access to or knowledge of the organisation's resources, including people, processes, information, technology and facilities.
Insider Risk	The likelihood of harm or loss to an organisation, and its subsequent impact, because of the action or inaction of an insider.
Insider Threat	An insider, or group of insiders, that either intends to, or is likely to cause harm or loss to the organisation.
Insider Event	The activity conducted by an insider, whether intentional or unintentional, that could result in, or has resulted in, harm or loss to the organisation.

The diagram below clearly visualises how the term ‘insider’ can be built upon;

Rationale for changing

Insider risk comes from everyone ‘inside’ your organisation

NPSA’s key message that we want to convey is that **if you have people, you have risk.** We therefore want all our customers to be **insider risk ready.** Our extensive and ongoing research indicates that harm or loss to an organisation could be as a direct result of unintentional activity from those with legitimate access, as well as from personnel who intend to exploit their access.

Being research led

It’s vital as an NTA we keep challenging our existing position. Following a rapid research review of literature, we found that most ‘insider’ definitions do not include exploitation or malice in the definition. The definitions usually relate to **access** rather than **exploitation**. Close Partners (e.g. CERT, US Government) similarly have also made recent changes to their definitions in a way aligns with NPSA’s forthcoming changes.

Developing a consistent lexicon

To date, NPSA has only communicated one definition which related to an ‘Insider’. This definition, however, failed to separate the community within which insider risk sits within and from those specific individuals that become an insider threat. This has resulted in language being utilised interchangeably and often in the wrong context. We want to change this, so we are all communicating in the same way.

Our next steps

Communications

NPSA Personnel & People Security Research & Development Team will be working alongside our communication colleagues to update existing guidance and products on our website to ensure it is consistent with this new terminology. Please bear with us whilst these changes are made. This document will be made available on the NPSA Website under the Insider Risk Page. We ask that NPSA customers refer to the revised definitions contained within this update.

Evaluation

It's vital we evaluate whether changes to NPSA's Insider lexicon results in greater clarity for our customers and supports you in understanding and mitigating this risk in a coherent way. We would welcome your feedback either via utilising the contact us form or providing feedback here.