CPNI
Centre for the Protection of National Infrastructure

Insider Threat in a Pandemic

PUBLISH DATE: Feb 2021

CLASSIFICATION: Official

An insider is defined as a person who exploits, or has the intention to exploit, their legitimate access to an organisation's assets for unauthorised purposes. This person could be a full or part time employee, a contractor, a volunteer, or even someone in your supply chain.

CPNI has conducted extensive research into insider threat and has identified common themes among the individuals and organisations involved. This note explains the key points that are relevant to mitigating the insider risk during a pandemic such at COVID-19.

Who

During COVID-19 you should be aware of:

- people deliberately trying to become a member of your workforce in order to conduct an insider act;
- an existing member of your workforce being coerced or recruited by a third party into conducting an insider act;
- an existing member of the workforce self-initiating an insider act for their own benefit;
- an ex-member of the workforce conducting an insider act after they have left;
- an existing member of the workforce being an unwitting insider by breaching your security policies and procedures without intentionally meaning to do harm, e.g. opening a phishing email.

What

The type of harm that can be inflicted by an insider act can include:

- national security damage, i.e. terrorism, espionage and cyber-attack;
- financial damage from the loss of assets including IP and sensitive data;
- operational damage by physical or cyber sabotage;
- reputational damage.

Organisations should specifically be aware of the risk of an insider making an unauthorised disclosure of sensitive information or the theft of physical assets relating to COVID-19, either to hostile foreign intelligence services, your business competitors, criminals, single issue groups or the media.

Personnel Security

Why

The reasons why people undertake hostile insider activity are complex and it is common to have more than one motivation. Financial gain is the most common primary motivation, and disgruntlement with the organisation will also be a significant factor. During COVID-19 there will sadly be people with hostile intent ready to take advantage of the crisis situation, particularly where staff may be working in unfamiliar environments, stressful personal circumstances, or in an atmosphere of job uncertainty.

How

CPNI research shows that there is a clear link between a hostile insider act taking place and exploitable weaknesses in the victim organisation's protective security and management processes. For example, during COVID-19 poor employment screening processes for employees and contractors could enable a deliberate insider who recognises the value in being able to legitimately access sensitive information, drugs, equipment.

A low level of line management oversight can enable an opportunistic insider to exploit their access to valuable assets because the early signs of counter-productive workplace behaviour are not spotted and acted upon. An organisation without strong leadership and communications at this time can quickly find staff are demoralised, disgruntled and more easily coerced into an insider act. This especially true where large numbers of the workforce are exiting the organisation or being 'furloughed'.

A strong security culture will provide a deterrence to insider activity by ensuring the workforce have a good level of security awareness, so are less likely to become unwitting insiders, and understand how to report concerns where they notice workplace behaviour of concern.

For further information and guidance on mitigating Insider Risk please go to:

https://www.cpni.gov.uk/insider-risks/insider-risk-mitigation-framework

The Home Office has issued guidance for how to conduct right to work checks during COVID-19 and this advice can also be applied to other parts of an organisation's screening processes where it is not possible to check an original document:

https://www.gov.uk/guidance/coronavirus-covid-19-right-to-work-checks