

# THE TRUSTED INSIDER THREAT

The trusted insider threat source category is one of the greatest security risks faced by Australian business.

The threat can be defined as a potential, current or former employees or contractors who have legitimate access to information, techniques, technology, assets or premises and intentionally or unknowingly assist external parties in conducting activities against an organisation.



Trusted insiders also commit malicious acts for self-interest; including financial gain or increased position and stature.

## The unintentional insider

Trusted employees or contractors who inadvertently expose, or make vulnerable to loss or exploitation, privileged information, techniques, technology, assets or premises. Inadvertent actions include poor security practices, such as leaving ICT systems unattended and failure to secure sensitive documents, and unwitting unauthorised disclosure to a third party.



## The malicious insider

Malicious insiders are trusted employees or contractors who deliberately and wilfully breach their duty to maintain security of privileged information, techniques, technology, assets or premises. There are two types of malicious insiders: self motivated or recruited.