Australian Government
Department of Home Affairs

CRITICAL INFRASTRUCTURE SECURITY CENTRE

Factsheet for Critical Infrastructure

Malicious Insider Risk

October 2025

Malicious insiders – those who have intent to cause disruption or harm to an organisation's functions or services – pose a significant risk, particularly for critical infrastructure. To mitigate this risk, critical infrastructure owners and operators should identify key assets and operations, as well as the personnel with privileged access to them.

This factsheet provides an overview of malicious insider risk, and includes considerations for its risk mitigation.

What is an insider threat?

An insider is anyone who has been given authorised access to an organisation's systems, facilities, information and/or other assets. This includes past and present employees, contractors (including in some instances third parties) and visitors.

Insiders' potentially harmful behaviour can be difficult to detect as they usually operate in legitimate roles with authorised access. This inside knowledge and access can result in far greater harm to infrastructure or operations than can normally be expected from outsiders.

An insider may be a dedicated, loyal worker one day, but dispositional changes can occur quickly if a real or perceived feeling of aggrievance forms. Trusted individuals do not necessarily require predisposition to criminal undertakings; opportunism, compounded by circumstance, may turn an otherwise trustworthy person into someone who seeks to deliberately steal, disrupt or harm an organisation and/or its assets.

Insiders either willingly, coerced or unknowingly exploited can also serve as a proxy for a business competitor or foreign power, using their legitimate access or knowledge to carryout harmful activities upon their behalf.

Digital environments

Digital services are an indispensable part of modern critical infrastructure operations. Digital environments can enable staff and contractors with trusted and privileged access to systems, networks, or information to intentionally cause harm. Malicious insiders may also attempt to leverage this access beyond the areas for which they have permission.

Artificial intelligence (AI) and social engineering

Technological advancement, particularly AI, can exacerbate the threat of social engineering as a means of compromising, disrupting, or extracting information. Malicious cyber actors use techniques such as social engineering to access accounts in order to exfiltrate sensitive information. Employees or contractors who become victims of social engineering can inadvertently become accidental or negligent insider threats. Advances in AI and its wide availability have increased the effectiveness of some of these approaches. Text, image and video communications are likely to be far more persuasive than in previous years, and credentials may be more convincingly falsified.

Physical access

Malicious insiders with authorised physical access to and knowledge of systems or infrastructure have the capability to inflict significant disruption or harm to those assets. Physical control systems are sometimes not well-equipped to defend against insider attacks, as emphasis is often placed on protecting and monitoring digital networks.

Malicious insiders with legitimate physical access and sufficient knowledge can cause prolonged outages, resulting in significant physical and reputational damage. For example, malicious insiders may tamper with operating systems, contaminate clean rooms, or damage facilities and equipment to cause more severe consequences.

Third parties

Third-party contractors and vendors represent a significant insider risk, as organisations increasingly outsource aspects of their operations to external providers. When the operational (OT) and information technology (IT) services of critical infrastructure operators are outsourced to contractors or vendors, they are often given the same privileged access to systems and networks as regular employees. However, these entities may present a higher risk than ongoing staff due to differences in onboarding processes, varying levels of security awareness and training, and inconsistent familiarity with organisational security protocols. Third parties are also attractive targets for threat actors, who may leverage or manipulate them to gain access to organisational systems.

Threat environment

Malicious insiders can manifest in various ways; however, most threats are associated with acts of espionage, sabotage, foreign interference, and theft.

Espionage

Malicious insiders may conduct espionage on critical infrastructure owners and operators in order to obtain corporate, sensitive or classified information. All information relating to Australia's critical infrastructure is of potential value and should be considered at risk.

Insiders may have legitimate access to such information, or they may obtain unauthorised access to additional systems and networks to exfiltrate information. Insiders can provide stolen information to different types of third-parties or may retain information for their own use or leverage.

Sabotage

Sabotage can include intentional physical or digital damage or disruption to critical operations and assets. Physical sabotage may involve damaging critical assets or equipment or even accessing a site to disrupt activity or render it obsolete. Cyber sabotage uses digital means to disrupt an entity's usual operations and delivery of critical services.

Foreign interference

Foreign interference can manifest when trusted insiders are enlisted by foreign governments (or foreign actors with links to governments) to undertake activities or actions against critical infrastructure that are counter-intuitive to Australia's national interests. An ability to interfere with how a critical infrastructure provider makes decisions and operates can achieve the aims of foreign powers and their proxies through the course of doing business.

Theft

Theft can take many forms, including fraud or intellectual property theft, typically motivated by financial gain. Any theft can compromise the functioning of critical infrastructure, cause loss of commercial advantage, sensitive information or research, and potentially impacting the operation of the asset.

Mitigating malicious insider risk

Critical infrastructure entities should develop mitigation strategies for malicious insiders that meet the requirements of their operations and security objectives. The following considerations may assist in guiding these ongoing risk mitigation efforts.

1. Target categorisation

Critical infrastructure operations present several attractive and opportunistic targets for a malicious insider, dependent on their motivations or goals. One approach for target categorisation is to consider possible targets under three broad categories: Information; Operational Infrastructure; and Financial.

- **Information** targets could include: employee information; corporate information; sensitive information; customer information; intellectual property; technical information.
- **Operational Infrastructure** targets could include: operational technology; information technology systems and networks; communication networks; data storage; power source and inputs; cooling systems; fuel storage; cabling and pits; security systems; logistics facilities and systems.

- **Financial** targets could include: financial accounts; trading accounts; hardware and software supply; raw materials.

2. Identifying critical workers

Insider risk is a human-centric issue. Developing a roles based understanding of managing the malicious insider threat can help identify differences in the level of risk posed by specific roles.

For critical infrastructure owners and operators, it is important to identify those critical workers who have significant control, access and understanding of their operations and services. By linking potential targets with the roles that have access and operational influence, organisations can identify in personnel-related security vulnerabilities and assess their potential impact on operations.

Control and management

Critical workers with substantial control or delegation over a critical component are attractive targets for malicious actors, as they can modify or remove parts of the component without additional oversight. Examples of these roles include:

- Executive staff and board members.
- High-delegation authorising officers.
- Inventory managers.
- High financial delegation.
- Procurement staff.

Privileged access

Personnel with access to critical sites, physical or digital systems, or control facilities can pose a risk due to their privileged access to assets.

The ability to access a target is a key factor in assessing an insider's potential intent and capability. Furthermore, legitimate access to one system can be leveraged across increasingly interconnected IT and OT networks. Examples of these roles include:

- SCADA control operators.
- ICT technicians.
- Third-party contractors.
- Privileged systems access.

Technical and procedural knowledge

Personnel with substantial knowledge of assets, systems, their architecture and operation, security procedures or personnel management can pose a risk due to the critical or aggregated nature of their expertise. For example, system operators/ administrators possess operational knowledge of systems and networks across an organisation.

These personnel could potentially identify where system vulnerabilities lie and pinpoint 'back-doors' into networks. Recent trends show that threat actors are increasingly targeting cloud workspaces and may focus on insiders who have detailed understanding of an entity's cloud and 'on-prem' environments. Examples of these roles include:

- System and network experts.
- IT architects.
- Facility managers.
- Terminal operators.

3. Understanding value of assets to malicious insiders

It is important for critical infrastructure owners and operators to identify which assets, information or physical sites represent the most attractive targets for a malicious insider. For businesses, the most predominate targets are usually personal and sensitive information, operational infrastructure (physical assets), and finance.

4. Risk management planning

The considerations outlined above align with requirements in the *Security of Critical Infrastructure Definitions Rules* (LIN 21/039) for critical infrastructure operators to identify critical components of their infrastructure and identify critical workers who are integral to the functionality of a critical infrastructure asset. Effective risk management plans allow operators to appropriately coordinate and allocate resources, funding and labour to mitigate insider risks.

Developing a better understanding of the likelihood and impact (identified through a risk assessment process) of an insider threat attack will support the risk prioritisation of insider threats within critical infrastructure. It will assist in correctly identifying how insider risks could manifest within a business. Once risk is understood, vulnerabilities that increase the likelihood of an insider risk occurring can be mapped.

Where can I find out more?

Within the Department of Home Affairs, the Critical Infrastructure Security Centre (CISC) drives an all-hazards critical infrastructure risk management regime in partnership with government, industry and the broader community. The CISC assists critical infrastructure owners and operators to understand the risk environment and meet their regulatory obligations. More information can be found on the CISC website or by contacting enquiries@CISC.gov.au.

The Critical Infrastructure Risk Management Program Guidance assists entities in understanding their obligations.

AusCheck provides fast, fair and reliable background checking services to Australia's most security-sensitive critical infrastructure sectors.

The Protective Security Policy Framework sets the Australian Government's minimum protective security standards.

The Australian Security Intelligence Organisation publishes available guidance on countering insider risk within entities.