

Defending from within: a guide to insider threat management

AUGUST 2026

77% of organisations have reported insider-driven data loss within the last 18-months. More than half of those experienced significant financial impact of greater than \$1 million.¹

Given how hard it is to protect against sophisticated cyber attacks by external threat actors, reducing insider risk can significantly affect an organisation's overall risk profile.

But insider threats present unique challenges for organisations:

- Malicious insiders have an advantage over external threat actors because they are not only aware of their organisation's policies, processes and systems, they are also aware of its vulnerabilities.
- On average, malicious insider attacks impose the greatest response costs when compared with other categories of attack vectors.²
- Technical tools that can be effective at preventing or detecting *external* threats are often insufficient to prevent *insider* threats—particularly when those insiders *already* have access to the at-risk information assets.
- The personnel screening techniques and monitoring tools that help to monitor and detect insider threats can present their own ethical, privacy, surveillance and employment law risks.

To better prevent, detect and respond to insider threats, organisations need to ensure close cooperation between their legal, HR, risk, IT, cyber and fraud functions, and adopt a combination of technical, operational and behavioural measures.

This guide is designed to help general counsel, HR, senior management and boards manage insider risks in a manner that is both legally compliant and ethical.

'Establishing and maintaining an insider threat mitigation program can assist an organisation to detect and respond to insider threats before they occur, or limit damage if they do occur.'³

Key takeaways



Significance of insider threats

Cyber events and insider threats are growing, making it more challenging for organisations to protect against such threats since insider threat actors often have an advantage, being aware of their organisation's policies, processes and systems vulnerabilities.



Cross-functional collaboration

To prevent, detect and respond to insider threats effectively, organisations need a combined effort from their legal, HR, risk, IT, cyber and fraud functions. A combination of technical, operational and behavioural measures should be adopted.



HR's role

Human resources plays a critical role in deterring, detecting and managing insider threats throughout the employment lifecycle. Recognising early warning signs generally requires insight into behavioural patterns that are more difficult to monitor using technical means alone.



Regulatory compliance challenge

The use of personnel screening and monitoring tools can present risks of their own. Organisations need to understand the regulatory risks associated with using these tools across the jurisdictions in which they operate.

Five questions boards should ask:

1

Who is accountable and responsible for managing insider risks?

2

Do we have a comprehensive and up-to-date insider threat management program?

3

How do we define insider threats?

4

What technical and operational controls have been or should be implemented to detect, monitor and reduce the risk of potential insider threats? How regularly do we review the adequacy of, and audit compliance with, these controls?

5

Do our cyber incident response playbooks and other preparedness activities (including simulations) contemplate insider threats?

What is an insider threat?

An insider threat occurs when any current or former employee, contractor, or board member maliciously or unintentionally misuses authorised access to workplace systems or information, causing potential harm to the organisation.⁴

The 'unintentional' insider

Unintentional insiders create insider threat risk through inadvertent actions, including poor security practices.

Accidental disclosure of data:
eg information sent to the wrong party or posted to a website.

Failure to secure sensitive data:
eg failing to ensure access to systems and/or documents is limited to those who have a need to know or failing to dispose of sensitive information securely.

Loss of physical records or equipment: eg paper documents or data storage devices such as data tapes, hard drives, laptops or smartphones.

Poor security practices:
eg forgetting to patch and upgrade.

The 'malicious' insider

Malicious insiders use their knowledge, access and position within an organisation to deliberately cause harm, loss or damage—either out of self-motivation, or where they have been recruited to assist a third party with malicious intent.

Sabotage: acts that impact an organisation's ability to function properly or that otherwise breach or expose an organisation's information technology infrastructure.

Fraud: unauthorised destruction, authorisation, concealment, falsification, alteration or misrepresentation of a business record with an intention to obtain a personal gain or cause a disadvantage; or theft of information that leads to an identity crime.

Theft: stealing an organisation's physical or digital information assets.

Violence: terrorism and workplace violence.

Espionage: spying or unlawfully accessing proprietary, confidential, commercially sensitive or national security information.

10 insider threat management best practices

Your insider threat management strategy should:

1 Be overseen by a cross-functional committee

The committee should comprise representatives from HR, IT, Security (physical and IT), Legal and Fraud. The board and risk sub-committee should endorse and oversee the program.

2 Address the organisational context in which malicious behaviours operate

A focus on individual behaviours—though important—will rarely be sufficient. Consider organisational cultural factors that might create insider dissatisfaction, as well as external risk factors (eg industry competition or malicious threat actors that might encourage or incentivise insider theft or misuse).

3 Cultivate a cyber-aware, no-blame culture (for mistakes)

Your people are your first and last line of defence. Staff should be encouraged to speak up as soon as they become aware of any actual or potential vulnerability or compromise, so that you can move swiftly to contain and mitigate any damage.

4 Be supported by policies and procedures assisting your organisation to identify, detect, respond to and recover from insider threats

These policies and procedures should be communicated to employees, and incorporated into employee and supplier onboarding, BAU training and termination processes.

5 Document, implement and audit technical and operational access controls

As a general principle, staff (and suppliers) should only have access to data and systems to the extent necessary for them to perform their roles. Access control protocols should outline *which* access controls should be applied in what circumstances; *when* they should be reviewed; *how* access will be monitored, logged and reported; *when* access rights should be revoked (eg when someone changes roles, leaves the organisation, or at a project's completion); and the *procedure* to be followed if there is an access control failure. The adequacy of these controls should be revisited, and compliance with them monitored and audited, on a regular basis.

6 Deploy behavioural monitoring and data loss prevention tools, supported by human input

Technical tools to monitor and identify anomalous behaviour (whether inadvertent or malicious) may include network monitoring software, identity and access management controls, and data loss prevention tools. Importantly, technical tools should be combined with effective oversight by human resources and IT to facilitate early detection, foster a security-minded culture and mitigate the vulnerabilities that human errors create.

7 Be designed and implemented with legal and ethical considerations in mind

Consider the privacy, surveillance and industrial relations implications of behavioural monitoring and sensitivity analysis tools and techniques, and related insider risk management controls—note that some of these regulatory requirements vary according to the state in which the relevant activities take place.

8 Include cybersecurity awareness and skills training

Negligent employee or contractor conduct now represents the fastest-growing category of insider risk—accounting for 53% of all insider cybersecurity incidents.⁵ Cybersecurity awareness and skills training is essential to help staff avoid certain inadvertent security breaches and detect potential risks before they arise.

9 Address insider threats (malicious and inadvertent) in incident response plans and cyber simulation programs

Your incident response team should consider in advance some of the unique issues that arise in managing insider threats. These include how the team may need to adapt its incident response plans and processes when dealing with a knowledgeable malicious insider.

10 Be reviewed on a regular basis (at least annually, and following any insider incidents)

This must be done to ensure the program remains fit for purpose.



HR's role: managing insider threats throughout the employment lifecycle

As the first and last point of contact for employees, HR performs a critical role in deterring, detecting and managing insider threats throughout the employment lifecycle.

While the tools, techniques and processes traditionally used to manage cyber threats can be effective at detecting or preventing external threats, they are often insufficient to detect or prevent insider threats.

Insiders have greater (and often legitimate) access to the valuable information held by organisations. This means that recognising the early warning signs of a potential insider attack generally requires insight into behavioural patterns and indicators that are more difficult to monitor and detect using technical means alone. For example, while an organisation may be able to rely on software to monitor for unauthorised access to its network by external third parties, or the potential exfiltration of its data, HR teams play an important role in monitoring personnel behaviour for issues that may indicate an insider threat risk.

HR teams are also uniquely placed to take the pulse of personnel within organisations because of their role managing personnel files and feedback. They often have access to information that enables them to identify patterns, and spot trends, assisting organisations in preventing or minimising the harm that insider acts and omissions cause.

*'Insider threat incidents cost organisations an average of US\$19.5M annually, up from US\$17.4M in 2024.'*⁶

*'The greatest risk often comes from ordinary employees making small but consequential mistakes.'*⁷

HR's role: managing insider threats throughout the employment lifecycle

Employment lifecycle checklist

Recruitment and onboarding

- ❑ **Background checks:** conduct background checks and other pre-employment checks (including qualification, reference and criminal history checks) to verify the applicant's identity and screen for red flags and potential negative indicators.
- ❑ **Deep fakes:** use tools to help detect the use of deep fakes to apply to a variety of remote work and work-at-home positions.
- ❑ **Monitoring and surveillance policies:** ensure new employees are aware of any monitoring and surveillance policies. Employees and contractors should be required to acknowledge and agree to these policies at the time they commence working at the organisation.

*'An organisation's employees are one of its most valuable assets and its most vulnerable cyberattack surface.'*⁹

Employment

- ❑ **Access controls:** implement and regularly update access controls (including after role changes and promotions) so that employees can only access information and systems to the extent necessary to perform their roles.
- ❑ **Individual credentials:** where possible ensure individuals are provided with their own (rather than shared) credentials, to aid in monitoring and detection of access to systems and data.
- ❑ **Training:** implement:
 - training for *all employees* to minimise the risk of inadvertent breaches (eg phishing attacks); and
 - *roles-based training* (including for HR and managers) to assist in identifying and monitoring employee behaviours that could be an indicator of insider threats (eg frequent policy violations, disruptive behaviour, financial hardship, job performance problems) (**key risk indicators**).
- ❑ **Monitoring tools:** deploy behavioural analysis and data loss prevention tools and policies (in consultation with IT and Legal). Regularly conduct IT security sweeps to identify unauthorised new software and malicious code that may have been introduced.⁸
- ❑ **Employee engagement programs:** implement employee engagement programs. Engaged and satisfied employees are less likely to pose an insider threat.
- ❑ **Policies:** monitor and enforce compliance with security, technology, confidentiality and privacy policies and procedures.
- ❑ **Early detection:** monitor, identify and report on potential problems (such as concerning behavioural changes) early on, including by creating a list of employees who are exhibiting key risk indicators.
- ❑ **Cyber simulations:** participate in cyber simulations involving insider threats.

Termination

- ❑ **Gardening leave:** consider requiring employees departing high-risk roles to go on gardening leave, restricting access to data and systems during that period.
- ❑ **Exit interviews:** conduct exit interviews, to provide departing employees with an opportunity to confidentially raise any concerns.
- ❑ **Termination policies:** enforce policies on termination of employment (including by requiring return or destruction of company information, and terminating or restricting access to premises and systems).

*'70% of insider threat incidents are completed within 60 days of an employee leaving the organisation.'*¹⁰

Spotlight: DPRK remote worker fraud – a state-sponsored insider threat

In recent years, state-linked cyber espionage activity associated with the Democratic People's Republic of Korea (**DPRK**) has become a pervasive threat, affecting hundreds of companies globally, including in engineering, technology, retail, crypto, fintech, and defence adjacent sectors. This industrial-scale fraud involves the use of remote IT workers placed within legitimate organisations to access sensitive data, steal intellectual property, disrupt operations, and generate revenue for the DPRK.

The Australian Signals Directorate (**ASD**) has co-signed multiple joint advisories with global partners and released an Advisory Note on the cyber risks associated with DPRK workers. Any Australian entity that unknowingly employs a DPRK-linked worker may be exposed to liability under Australia's autonomous sanctions regime.

In recent months, other state-linked actors and transnational organised crime groups have been observed adopting similar remote worker infiltration tactics, leveraging the same playbook of fabricated identities, AI-assisted interviews, and laptop farm infrastructure to place operatives within target organisations and circumvent sanctions and criminal background checks.

How the scheme works

- 1 DPRK operatives create false profiles using stolen or fake personal information and apply for high-paying, remote roles.
- 2 Operatives use AI or other remote assistance to pass interviews, coding assessments, and background checks for remote roles.
- 3 Once hired, operatives request company issued laptops be sent to physical addresses controlled by facilitators outside the DPRK. The devices are then held in laptop farms managed and remotely accessed by or on behalf of DPRK operatives.
- 4 In some cases, the DPRK operative will perform the job themselves, in other cases they outsource tasks to a third party.
- 5 Their salary is sent back to fund the North Korean regime, which also weaponises IP and other sensitive corporate information accessed as part of the fraud.

The risks

Beyond salary-based revenue generation, affected companies face broader risks including data theft, malware installation, insider access abuse, and potential sanctions violations.

*'It is estimated DPRK cyber actors and IT workers have stolen over USD \$2.8 billion in cryptocurrency since January 2024 and earned an estimated USD \$300-800 million in revenue in 2024.'*¹¹

What to do if you detect or suspect that a worker may be a DPRK worker

- 1 Contact the Australian Sanctions Office and suspend all future payments until further direction.
- 2 Limit access to corporate systems and data.
- 3 Thoroughly investigate what has been accessed, and whether any authorised software has been uploaded, or malicious code has been inserted into existing programs

For more information on the red flag indicators that may suggest you're recruiting a DPRK worker and what to do about it, see:

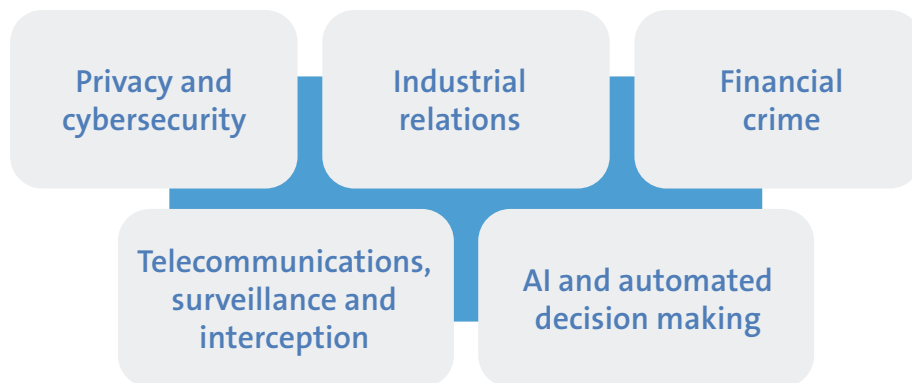
- [Advisory note DPRK information technology workers](#), 31 July 2026.
- [Joint statement on DPRK IT workers | Australian Government Department of Foreign Affairs and Trade](#), 31 July 2026.
- [Cyber risks of DPRK IT Workers](#), 6 November 2025.

*'We urge all countries, companies, and other entities to deepen their understanding of North Korean IT worker schemes and implement measures to counter the tactics... Companies operating online platforms should continue to strengthen their countermeasures, such as enhancing identity verification procedures (strict review of identification documents, requirement of in-person interviews, etc.) and detecting suspicious accounts (introduction of systems that notify anomalous information entries, etc).'*¹²

The compliance challenge: personnel screening and monitoring

Personnel screening and monitoring tools are critical to the success of insider threat management programs because they enable organisations to rapidly detect and respond to such threats. But these tools can present risks of their own. Organisations (and, in particular, HR and IT teams) need to understand the regulatory risks associated with using monitoring tools across the jurisdictions in which they operate.

Consider these regulatory regimes



When implementing and utilising screening tools and techniques, it's important to be aware of the various regulatory requirements. They vary significantly across jurisdictions (and even, in some cases, from state to state). Some jurisdictions are reasonably permissive, whereas others require consultation with local regulators, consent and other strict compliance measures (eg there are particularly prescriptive requirements in the European Union and the United States).

Organisations looking to deploy these tools across multiple jurisdictions need to decide whether to adapt the use of those tools for each jurisdiction, implement a global program or adopt a hybrid approach.

Common screening and monitoring tools and techniques



Pre-employment screening and background checks, including ID verification and qualification, reference and criminal history checks.



Data loss prevention (DLP) software that enables an organisation to monitor employee communications to ensure personal and other confidential information is not sent outside it.



User behaviour analytics: uses AI, machine learning, and deep learning to detect abnormal or risky patterns of behaviour across users, machines, and other network entities, helping identify potential insider threats.¹³



Full packet capture: an after-the-fact investigative capability that other security tools can't provide—its uses include capturing malware samples, network exploits and determining if data exfiltration has occurred.



Other tools that enable organisations to monitor and control **system access**.

The compliance challenge: personnel screening and monitoring

Ask these questions before deploying personnel screening, behavioural monitoring and DLP tools

1 Do we need to undertake a risk assessment?

Tip! Even if you don't think you need to, you should! Your risk assessment should identify (among other things) the objective of the tools or program, plus the guardrails, relevant compliance and ethical considerations, and controls to be implemented to mitigate regulatory and other risks.

2 Is it legal?

Tip! Consider whether there are any laws that prohibit or restrict you from monitoring personnel's communications or activities (eg laws governing privacy, record retention and destruction, interception, surveillance, employment relations and automated decision making, as well as sector-specific laws). Are there any exceptions that might apply?

3 Do we need to tell anyone or get their consent? Are we *permitted* to notify in the circumstances?

Tip! Consider whether you are required to publish an internal and/or external policy, or otherwise notify personnel or relevant third parties (eg recipients or senders of monitored communications who are not employees) about the proposed monitoring activity. Consider also prohibitions against 'tipping off' in relevant circumstances.

4 Do we need to notify or get approval from a regulator in order to deploy these tools?

5 Are we outsourcing this activity? Does the proposed outsourcing align with our supplier management policy?

Tip! Consider what due diligence you need to undertake, and what technical and operational controls the supplier should be required to apply.

6 Do we need to update any statements or representations that we currently make (to personnel or relevant third parties) so that they reflect the proposed activity?

Tip! Ensure that any statements made in connection with the proposed monitoring activity are not misleading or deceptive.

7 How long can (and should) we keep screening and monitoring data?

Tip! Consider whether your record retention and destruction policy adequately addresses personnel screening and monitoring data (eg whether you need to retain copies of underlying ID verification documentation once the employee's identity has been verified).

8 Who needs access to the screening and monitoring data? What access controls should be applied?

9 How will the screening and monitoring data be protected?

10 What other key issues or red flags do we need to consider?

Tip! Consider upcoming regulatory reforms (eg Privacy Act reforms, new AI regulation).

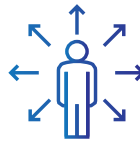
AI occupies a dual role in contemporary cyber risk: it can be exploited by threat actors, while simultaneously strengthening organisations' ability to comply with security and privacy obligations. Entities that made extensive use of AI-based detection and automated response tools recorded average breach costs of US\$3.62 million, compared with US\$5.52 million for organisations that did not deploy such technologies.¹⁴

Conducting internal investigations into insider threats

Insider risk checks



Consider the purpose of the investigation (eg for the purpose of the organisation obtaining legal advice) and ensure it is conducted in accordance with its stated purpose.



Involve internal and external experts to ensure that all potentially relevant evidence, including the sources of that evidence, are identified, collected, properly analysed and understood and that the integrity of any such material is maintained at all times.



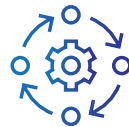
Don't delay but do not act in haste—a well-planned but timely investigation is critical.



Ensure compliance with all policies and procedures relevant to the investigation and the matters being investigated, including relating to workplace surveillance and privacy.



Consider suspending employees on full pay pending investigation and removing access to information and systems—the nature of the matters being investigated may require this.



Ensure sufficient and appropriate resources are committed to the investigation so that it can be conducted efficiently and thoroughly and is also capable of withstanding internal and external scrutiny.



Assess what evidence should be collected before the relevant employees are informed of the investigation.



Establish a clear document management protocol so that all records obtained or created during the investigation are appropriately handled and stored. Ensure that any records that are created are accurate, contemporaneous, and appropriately categorised (eg confidential and privileged, commercial in confidence, etc.).

*'Even the most secure organisations can face devastating losses caused by a knowledgeable and motivated insider who is not contained by adequate internal safeguards or sufficiently rigorous administrative standards and expectations.'*¹⁵

Contacts



Valeska Bloch

Partner and Head of TMT and Cyber
T +61 2 9230 4030
Valeska.Bloch@allens.com.au



Sonia Millen

Partner, Employment & Safety
T +61 2 9230 4304
Sonia.Millen@allens.com.au



David Rountree

Partner
T +61 7 3334 3368
David.Rountree@allens.com.au



Isabelle Guyot

Partner
T +61 2 9230 4752
Isabelle.Guyot@allens.com.au

Allens is an independent partnership operating in alliance with Linklaters LLP. 19993D

Endnotes

- 1 Fortinet / Cybersecurity Insiders, [Insider Risk Report](#) (October 2025).
- 2 IBM, [Cost of a Data Breach Report 2025](#) (2025).
- 3 Australian Signals Directorate, [Guidelines for Cyber Security Incidents](#) (17 March 2026).
- 4 AUSTRAC, [How Resistant is Your Business to Insider Threats?](#) (15 December 2025).
- 5 Ponemon Institute / DTEX, [Cost Of Insider Risks 2026 Global Report](#) (2026).
- 6 Ponemon Institute / DTEX, [Cost Of Insider Risks 2026 Global Report](#) (2026).
- 7 Fortinet, [2025 Insider Risk Report: The Hidden Cost of Everyday Actions](#) (16 October 2025).
- 8 Department of Foreign Affairs and Trade, [Cyber risks of DPRK IT Workers](#) (6 November 2025).
- 9 Isaac Kohen, [Five Steps to Secure an Enterprise Against Insider Threats](#) (March 2024).
- 10 SecureWorld, [Identifying Insider Threats: How Human Resources Can Help](#) (15 July 2018).
- 11 Department of Foreign Affairs and Trade, [Combating DPRK Remote IT Worker Threats](#) (30 March 2026).
- 12 Department of Foreign Affairs and Trade, [Joint statement on DPRK IT workers](#) (31 July 2026).
- 13 Exabeam, [UEBA \(User and Entity Behavior Analytics\): Complete 2025 Guide](#) (2025).
- 14 IBM, [Cost of a Data Breach Report 2025](#) (2025).
- 15 Securities Industry and Financial Markets Association, [Insider Threats Best Practices Guide, 3rd Edition](#) (July 2018).

Read more on this topic at
allens.com.au/cyber