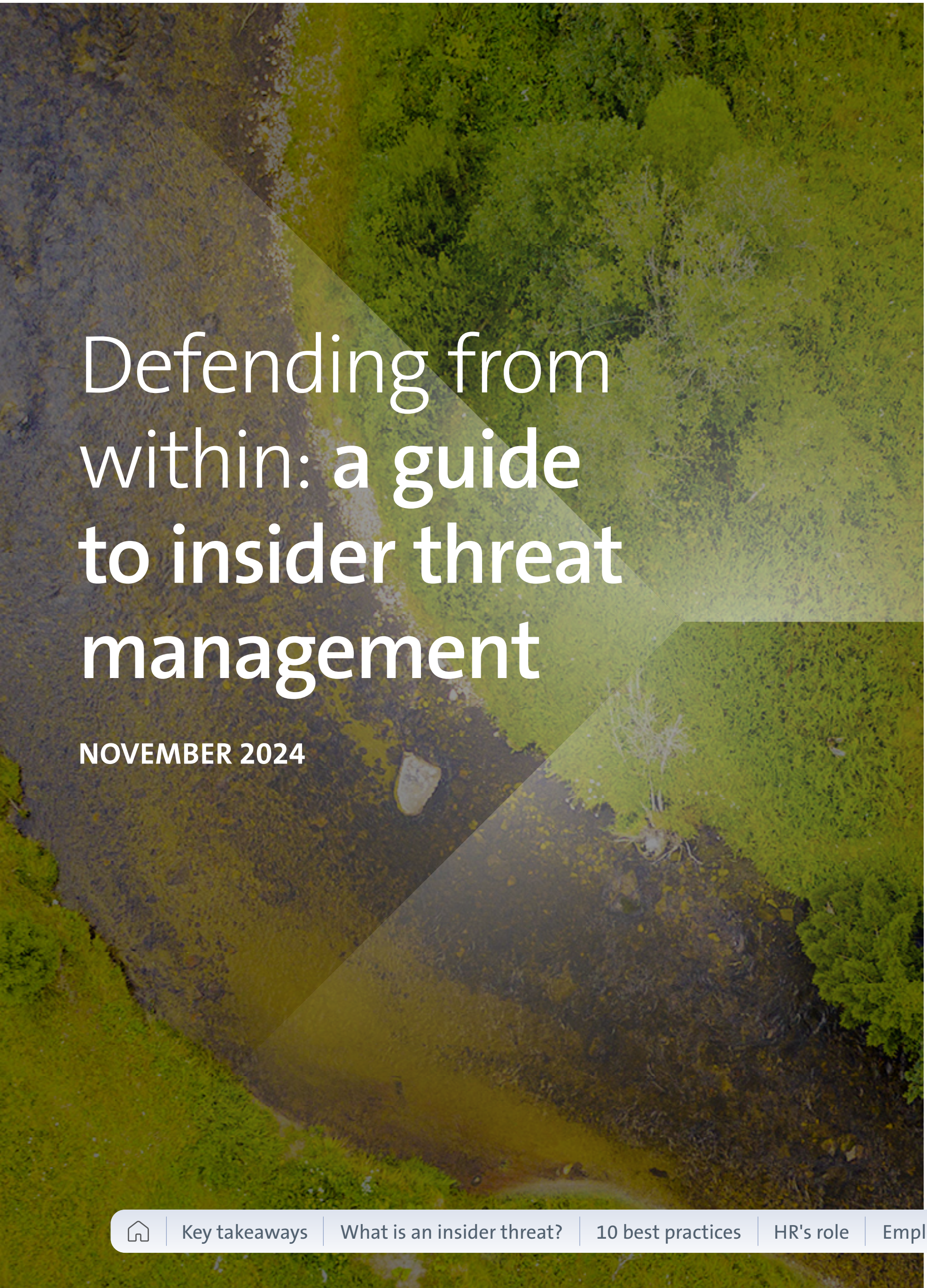
Allens

In alliance with Linklaters



Defending from within: **a guide to insider threat management**

NOVEMBER 2024

More than 35% of all cyber events globally originate *inside* an organisation—either as a result of error or misuse. This number is growing.

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, the costs incurred in responding to a malicious insider attack are the highest of all attack vectors.[1]
- 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.

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.

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.

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.

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

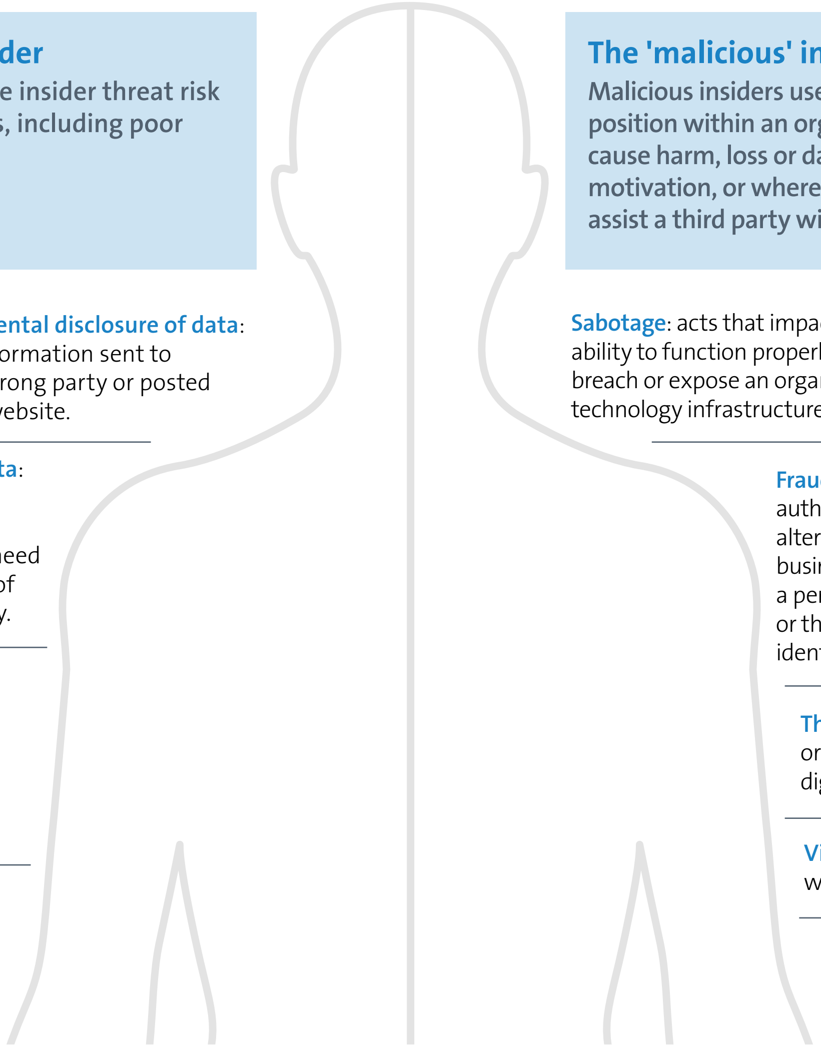
What technical and operational controls have been or should be implemented to detect, monitor and reduce the risk of potential insider threats? How regularly do we review the adequacy of, and audit compliance with, these controls?

5

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

What is an insider threat?

An insider threat is any current or former employee, contractor or business partner who unintentionally or maliciously uses their access to an organisation's assets (whether physical or digital) in a way that could cause harm to the organisation or its workforce.[2]



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

More than half of cyber incidents that are the result of insider threats arise due to employee or contractor error.[3] 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.

> *'Large organisations with a headcount of more than 75,000 spent an average of $24.60 million over the past year to resolve insider-related incidents. To deal with the consequences of an insider incident, smaller-sized organisations with a headcount below 500 spent an average of $8 million.'*[4]

Recruiting deepfakes

The FBI Internet Crime Complaint Center has, over the past two years, warned of an increase in complaints reporting the use of deepfakes and stolen personal information to apply for a variety of remote work and work-at-home positions. These positions include information technology and computer programming, database and software jobs that would provide access to critical systems and data.

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.'*[5]

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).

□ **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.

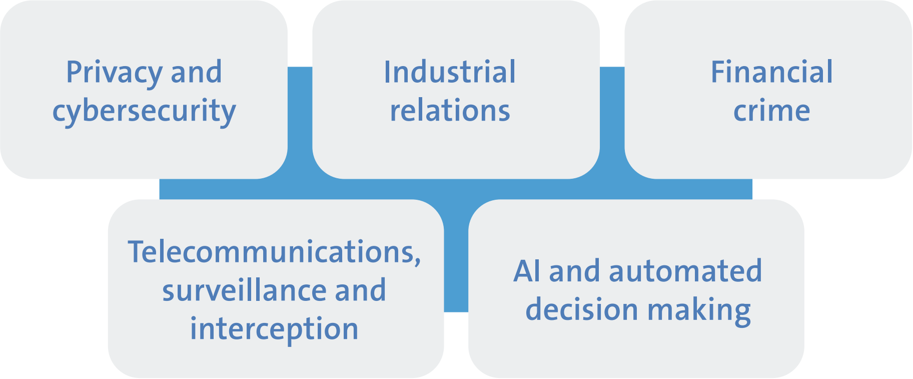
□ **Termination policies:** enforce policies on termination of employment (including by requiring return or destruction of company information, and terminating or restricting access to premises and systems).

> *'70% of insider threat incidents are completed within 60 days of an employee leaving the organisation.'*[6]

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


Privacy and cybersecurity
Industrial relations
Financial crime
Telecommunications, surveillance and interception
AI and automated decision making

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: which involves the use of AI to analyse trends across large datasets, to identify patterns of behaviour that may indicate security breaches, data exfiltration or any other malicious activity that might otherwise go unnoticed.[7]

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).

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.

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

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.

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

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.

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

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.

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.’*[8]

Contacts

Valeska Bloch
Partner and Head of 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

Gavin Smith
Partner and Co-head of Corporate, Head of Technology, Media and Telecommunications
T +61 2 9230 4891
Gavin.Smith@allens.com.au

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

Phil O'Sullivan
Partner
T +61 2 9230 4393
Phil.O'Sullivan@allens.com.au

Jessica Mottau
Partner
T +61 2 9230 4587
Jessica.Mottau@allens.com.au

Elyse Adams
Partner
T +61 3 9613 8534
Elyse.Adams@allens.com.au

Dominic Anderson
Partner
T +61 2 9230 4099
Dominic.Anderson@allens.com.au

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

Endnotes

1 IBM, Cost of a Data Breach Report 2024 (July 2024).
2 See Daniel Cost, CERT Definition of 'Insider Threat'—Updated (March 2017) and Cybersecurity and Infrastructure Security Agency, Human Resources' Role in Preventing Insider Threats.
3 Ponemon Institute, 2023 Cost of Insider Risks Global Report (2023).
4 Ponemon Institute, 2023 Cost of Insider Risks Global Report (2023).
5 Isaac Kohen, Five Steps to Secure an Enterprise Against Insider Threats (March 2024).
6 Identifying Insider Threats: How Human Resources Can Help (secureworld.io).
7 CyberArk, What is User Behaviour Analytics?.
8 Securities Industry and Financial Markets Association, Insider Threats Best Practices Guide, 2nd Edition (February 2018).

New cyber incident response obligations for Australian organisations

Balancing act: establishing and preserving legal professional privilege in a cyber incident

AICD's guide for directors on governing through a cyber crisis

Why organisations must embed mental health and wellbeing support into cyber incident response planning

Why every company should have a structured cyber simulation program

A step-by-step guide to assessing compromised data after a cyber incident

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