



Australian Government

# THE INSIDER THREAT TO BUSINESS

A personnel security handbook





*The Hon Nicola Roxon MP  
Attorney-General*

## MINISTERIAL FOREWORD

Business plays a crucial role in Australia's social and economic wellbeing.

But what if a business was disabled for a length of time? What would be the impact on its profitability, service delivery, employees, and the flow-on effects to the broader community? What would be the key to the business returning to normal operations quickly?

There are a range of threats or hazards, such as natural disasters and equipment failure, that can disrupt or disable business operations.

This booklet deals with one particular threat – the 'insider' – a person committing a malicious act or causing harm.

While malicious acts by insiders are rare, the potential level of threat warrants alertness by business.

In Australia, insider actions have historically been for personal gain or corporate or state-sponsored espionage. Internationally, however, there have been incidents of insider activity for radical and ideological purposes, sometimes furthered by terrorist means. To help illustrate insider activity, this booklet contains some case studies that are based on true stories from around the world.

Whatever an insider's motivations, their activity can be harmful, expensive, embarrassing and disruptive. It can also have long-term detrimental effects on business operations, profitability, reputation and culture.

While most insider activity is likely to be for personal gain, it is wise and sensible to protect your business against the full range of insider threats.

This is part of building the resilience of your business – managing both foreseeable and unforeseen or unexpected risks.

This booklet outlines how you can make your business more resilient to insiders by understanding the threat and evaluating the risks, so you can develop a personnel security framework.

Good personnel security is good business – it's also smart business.

I encourage all business owners to read this booklet – not only to help maintain your competitive edge and profitability – but also to help protect the broader community from the threat of insiders.

UNDERSTANDING THE INSIDER THREAT – Who, what, why, how and when

Definition

The insider threat can be defined as:

*one or more individuals with the access and/or inside knowledge of a company, organisation, or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm.*<sup>1</sup>

Who

An insider is someone who is a current or previous worker of an organisation or has legitimate access to its resources and uses or attempts to use that access to cause harm. This includes past and present employees and contractors. The insider may be someone who:

- deliberately seeks employment with an organisation with intent to cause harm
- causes harm once employed but who had no intention of doing so when first employed, or
- is exploited by others to do harm once employed, and may be either a passive, unwitting or unwilling insider.

What

Insider activities can range from active betrayal to passive, unwitting or unwilling involvement in causing harm. They may include such things as:

- unauthorised disclosure of information
- physical or electronic sabotage

- facilitating third party access
- financial or process corruption, and
- theft.

Why

There are complex reasons why an employee would deliberately seek to cause harm.

An insider will usually be motivated by one or a combination of reasons. A useful acronym to understand the motivations underlying the willing behaviour is **crime**

- **coercion** – being forced or intimidated
- **revenge** – for a real or perceived wrong
- **ideology** – radicalisation or advancement of an ideological or religious objective
- **money** – for illicit financial gain, and/or
- **exhilaration** – for the thrill of doing something wrong

It is important to note that many employees with motivation and malicious intent never commit an act of betrayal.

How and when

Insiders will identify and understand the business' vulnerabilities and know how and when they can be exploited.

They will use the trust invested in them, and their subsequent access to resources and facilities, to harm the business. They may either abuse legitimate access or take advantage of poor access controls to gain unauthorised access.

These activities may take place after considerable planning or on the spur of the moment when an opportunity arises.

<sup>1</sup> Noonan, T. and Archuleta, E. (2008) 'The National Infrastructure Advisory Council's Final Report and Recommendations on the Insider Threat to Critical Infrastructures'

SCENARIO 1

Melissa, 36, had worked for a small pharmaceutical laboratory for 12 years, almost since its inception. She was well known and well liked, mostly because she was good fun. Everyone knew she liked the local clubs for a drink and a dabble on the pokies.

In January, Melissa came back to work from Christmas holidays less lively than normal. Word got out that she had separated from her husband. Over the next few months Melissa's demeanour and behaviour changed; she often arrived late and left early, she was distracted and took a lot of calls outside on her mobile phone. Everyone put this down to the separation.

One weekend the laboratory was burgled and a large volume of a chemical used to produce methamphetamines was stolen. There appeared to be no sign of forced entry. Melissa called in sick that week, but no-one took too much notice.

The following week, Melissa was arrested. The CEO of the company called a staff meeting to explain that Melissa had amassed a serious gambling debt and in the process dealt with a well known criminal network. She wasn't able to repay some of her debt and, with her and her family's safety under threat, had provided access to the thieves.

The CEO told staff that Melissa was very apologetic and upset when interviewed by police. She also said she had tried to send signs to a few colleagues that she was in trouble as she was too scared to tell anyone directly. She pleaded guilty and was sentenced to six months in prison. Her husband took custody of their three children and their house was sold to repay some of the debt. The chemicals were not recovered, although police had three suspects and were continuing their investigation.

- ✕ note significant changes in an employee's personal circumstances
- ✕ note when an employee seems under considerable stress
- ✕ check whether all employees need after hours access



PERSONNEL SECURITY – What it is and why do you need it?

Personnel security is a security framework or a set of measures to manage the risk of an employee exploiting their legitimate access to an organisation's facilities, assets, systems, or people for illicit gain, or to cause harm.

Implementing a personnel security framework will help you build an understanding of any insider threats facing your business and give you the tools to manage any associated risks. It will also allow you to place a level of trust in your employees so that you can confidently give them access to your business.

A Personnel Security Framework

PERSONNEL SECURITY PLAN		Page No.
Organisational personnel security	Know your business	5
	A good security culture	5
	A personnel security risk assessment	6
	Understanding the legal framework	6
	Communicating personnel security to your employees	6
Pre-employment personnel security	Identity checks	6
	Overseas applicants or applicants who have spent time overseas	7
	Qualification and employment checks	7
	National criminal history check	8
	Financial background checks	8
	Document security	8
Ongoing personnel security	Access controls	8
	Protective monitoring	8
	Security culture	8
	Countering manipulation	8
	Reporting and investigation	9
	Ongoing checks	11
	Contractors	11
Information and communications technologies	Access controls	12
	Shared administrative accounts	12
	Account management policies and procedures	12
	Standard operating environment	12
	Logging and monitoring	12
	Employee understanding of the consequences	12

Organisational personnel security

Know your business

You know your business best; its key roles and key people, its strengths and its weaknesses, its environment and its operations.

When developing your personnel security framework take into account:

- the broad operational environment
- your risk management framework
- the key positions of trust in your organisation
- the reliability and integrity of your recruitment processes
- your human resource structure and processes
- the interaction between your human resource and protective and electronic security areas, and
- implications of incidents which result from a breach of personnel security.



A good security culture

A good security culture is vital. It will include most, if not all, of the following characteristics:

- awareness: the security risks for the organisation are understood and accepted by employees
- ownership: security is viewed as an integral part of the organisation's business
- reporting: security breaches are reported and reporting is accepted as normal by employees
- compliance: there is a high level of compliance with security policies and procedures
- discipline: sensitive access or information is not provided unless there is a clear requirement
- challenge: employees are confident to challenge others if they are not complying with security requirements
- communication: the rationale for security measures is clearly communicated to all employees
- senior sponsorship: senior managers place, and are seen to place, a high value on security
- enforced disciplinary procedures: security breaches are dealt with consistently and rigorously, according to well established guidelines, and
- offering incentives: the generation of ideas for improving security and reporting security breaches is rewarded appropriately.<sup>2</sup>

<sup>2</sup> Personnel Security: Threats, Challenges and Measures (2007) Centre for the Protection of National Infrastructure [www.cpni.gov.uk](http://www.cpni.gov.uk)

A personnel security risk assessment

Most businesses have implemented basic risk management principles. These same principles apply when developing your personnel security framework. Based on your risk assessment you will be able to:

- prioritise risks to your business
- develop a personnel security plan, identifying security measures to mitigate the risks
- allocate resources cost effectively and commensurate with the risk, and
- communicate insider risks to managers and employees and secure their engagement in your personnel security framework.

Understanding the legal framework

Understanding the legal framework is vital. When developing your personnel security plan, you will need to be aware of a wide range of legal issues. If you have any concerns or questions, it is wise to seek legal advice to make sure your framework and processes comply.

Relevant legal issues include:

- general discrimination, including race, gender, religion, sexual orientation, age and disability
- criminal history
- immigration status
- handling personal information
- privacy, and
- occupational health and safety.

Communicating personnel security to your employees

Background checking is designed to give you confidence that prospective employees are who they say they are and have the skills and experience they say they do.

In turn, this will provide you with the requisite level of trust in a prospective employee to offer them a job and give them access to your business and its resources.

As early as possible in your recruitment process advise all applicants about:

- your business’ requirements for pre-employment checking
- why those checks are conducted
- what your business will do with the information collected
- to whom the information might be disclosed, and
- what subsequent decisions will be made about the applicants’ suitability for work.

With all pre-employment background checks, be sure of the criteria for checking before you start. Identify the requisite level of checking for each position.

The more sensitive the position, the more checks you will probably want to make.

Pre-employment personnel security

Identity checks

Verifying the identity of applicants during recruitment is fundamental. It will give you a level of assurance about your prospective employee.

Details on how to verify the identity of potential employees can be found in Australian Standard AS 4811-2006 *Employment Screening and HB 323-2007 Employment Screening Handbook*.

These publications can be found at [www.saiglobal.com](http://www.saiglobal.com)

Overseas applicants or applicants who have spent time overseas

Many prospective employees will have lived and worked outside Australia. For Australian citizens who have lived and worked overseas you should try, to the extent possible, to conduct the same checks you would if the applicant had worked only in Australia.

For non-Australian citizens, in addition to the checks you would conduct for an Australian citizen you should also check whether the applicant has the right to work in Australia, in what positions and for how long.

Qualification and employment checks

You should check the details in an applicant’s curriculum vitae to ensure there are no unexplained gaps or anomalies. Where possible you might also like to contact previous employers to confirm past employment and ensure that the details match those in the applicant’s CV.

You may also wish to contact previous employers for a character reference.

When confirming an applicant’s qualifications you should:

- request original certificates or certified copies
- compare details with those provided by the applicant, and
- confirm the existence of the institution and confirm the details provided by the applicant.

SCENARIO 2

Peter, 49, had worked as an accountant in a medium sized company in the telecommunications sector for two years. He was known to be competent, quiet and unassuming and fitted neatly into most people’s stereotype of the quiet accountant.

Peter’s boss, the Chief Financial Officer, was head hunted to a larger firm and Peter was promoted to his job. It was a young company and had made a lot of money quickly. The CEO was an ideas man and he trusted Peter to look after the money side of things. Ten months after Peter took over as CFO regulations changed and five new businesses entered the market. Peter informed the CEO and executive that, although still profitable, the company’s profits were likely to be under the forecast. Some people noticed that Peter was driving an expensive new car.

Four months later, Peter left the company suddenly. Within days, the CEO was told that the company was in deep financial trouble. Twenty staff were made redundant that day, with the remaining 110 told their future was shaky. A consulting accountant quickly found that Peter had stolen nearly two million dollars from the company and had hung on to the very last minute before it all came crashing down. The matter was referred to the police.

Peter could not be tracked down, but police soon found that he had given a false name to the company when he was recruited and most of the details on his CV were either misleading or false. Police discovered his true identity but unfortunately Peter had left the country.

- ☒ check identity
- ☒ check qualifications
- ☒ notice significant unexplained changes in an employee’s circumstance



National criminal history check

If you conduct a criminal history check you should be clear about what convictions would preclude a person from employment.

You should be aware of the provisions of the relevant jurisdictional spent conviction scheme. You should also bear in mind that just as a criminal conviction is not necessarily a bar to employment, neither does a clean record guarantee that a person will not present an insider threat to your business.

If you choose to do a criminal history check, it should be undertaken by either the relevant police service or an authorised agency. You will need the applicant to complete a consent form to have the check undertaken.

Financial background checks

You may consider conducting a financial background check or request details of an applicant's financial position. As with all pre-employment checks, the applicant should be advised of the reason for the check.

Financial background checks can be conducted by a credit checking agency. Again, you will need the applicant to complete a consent form to have the check undertaken.

Document security

In the case of any pre-employment check, you should ensure that all documentation is securely held and made available only to those who can demonstrate a need to access the information.

If an applicant fails to meet the standards that your business (and/or legislation) has set and their application is rejected, they should be advised of the grounds for rejection and informed of any available avenues of appeal.

Ongoing personnel security

Access controls

Access controls, manual or automated, protect your business from unauthorised access to its physical, human or electronic assets. Giving appropriate access to those you trust is an important element of your personnel security framework.

Security passes are the most common form of physical access control. Most passes today contain a photograph and could also include information about the level of access and security clearance held by the bearer. This could be colour coded to help other staff determine whether a person is authorised to be in a certain area or access certain material. You should issue passes from one single location or department to reduce the possibility of duplication or confusion.

Protective monitoring

Your physical access controls should have a system that enables you to monitor any breaches or attempted breaches.

For particularly sensitive areas you may choose to use a system that provides real-time alerts about unauthorised access. You may choose to install more intensive monitoring, such as security staff or closed circuit television (CCTV) at certain access points.

The more layers of security you add the more likely you will identify unusual behaviour.

Security culture

Countering manipulation

There may be signs that an employee is vulnerable to becoming an insider.

It is important to note that these signs are of general stress and do not necessarily indicate a propensity to become an insider:

- appearing intoxicated or affected by a substance at work
  - increased nervousness or anxiety
  - decline in work performance
  - extreme and persistent interpersonal difficulties
  - extreme or recurring statements demonstrating a level of bitterness, resentment or vengeance
  - creditors calling at work
  - sudden and unexplained wealth, and/or
  - inappropriate interest in sensitive or classified information.
- *benefit of the doubt*: in many cases there may be a simple explanation for a security breach, so where possible give the employee the opportunity to explain. Where this is not possible, you should consider when to inform the employee they are the subject of an investigation
  - *criminality*: report any suspected criminal activity to the police as soon as possible
  - *legality*: handle all internal investigations legally, and
  - *morale*: be aware that an investigation, even one handled well, can have an adverse impact on employees.

Your employees should be educated in recognising the signs of insider behaviour. They also need to be made aware of the potential that they could be recruited by someone from outside the business who may:

- ask seemingly innocent questions about the organisation in a piecemeal way, or
- ask colleagues to overlook small security breaches, such as being in an unauthorised area or not wearing a security pass.

Although each activity may seem insignificant, they may be highly valuable to an adversary when put together.

Reporting and investigation

Suspected breaches of any personnel security measures could be reported in a number of ways.

You may choose to use existing lines of reporting, or you may consider establishing an alternative mechanism such as an informal network or a reporting hotline. In either case reports should be investigated quickly to ensure confidence in your personnel security measures is maintained.

If you conduct an in-house investigation you should follow some general principles:

- *guidelines*: establish guidelines (if they do not already exist) about how an investigation will run, how evidence will be gathered, how witnesses will be approached and who will run the investigation



SCENARIO 3

George, 24, worked for a large company in the resources sector. He had been in Australia for six months, from Europe. Although quiet initially, he soon started talking about starving people and weather changes that would cause massive tsunamis that would drown half the world.

George’s workmates wondered why he worked for the company; he didn’t seem interested in the good wages and he didn’t seem to approve of digging into the ground for valuable resources. This wasn’t something they thought much about, but they did notice their supervisor treated George’s talk with derision.

One morning George’s colleagues arrived to find the companies equipment spray painted, its tyres slashed and engines clogged with sand. They also found George and two friends chained to a mine entrance, with what they said were bombs in their backpacks. George demanded the company cease operations immediately and give 80 per cent of last year’s profits to charity. He said the company was committing environmental terrorism.

After hours of negotiation the police removed George and his friends. While they discovered the bombs were crude hoaxes, the company lost over \$4 million in damaged equipment and lost operating time. The company then spent \$1.25 million on an immediate upgrade to its security and lost 4 per cent of its share value as investors

lost confidence in management. George and his friends were each tried, convicted and sentenced. During the course of the trial it was revealed that George was a well-known environmental activist in his homeland and had sought to work at the company with the intention of sabotaging its operations.

- ✗ check identity
- ✗ note strongly held views that seem to contradict the purpose of the business
- ✗ managers should demonstrate respect for their employees’ views (unless they are discriminatory) even if at the same time holding and expressing concerns to other managers
- ✗ check whether all employees need after hours access



Ongoing checks

Employers might also want to think about whether they would like to repeat any of the pre-employment checking stages when an employee applies for a promotion or at regular intervals while in their employment.

Contractors

Contractors pose additional challenges, however they should be included in your personnel security framework to the extent possible.

Where you are unable to carry out background checks to the same level as employees because of time constraints, or lack of full information, you should be aware of the associated risks and know what you need to do to manage these risks.

If you have identity and/or access control passes it is a good idea to have an identifier to indicate a contractor. It will be very important to ensure that once the contract has finished the contractor returns all access cards.

SCENARIO 4

Jane had been working as a system administrator for a large company for several months. She was competent and considered a hard worker.

During a corporate restructure, Jane’s roles were changed. Jane started to voice her objections to the changes, and the quality of her work started to deteriorate. During office relocations, Jane was moved from a desk within the centre of her work area to the edge. Shortly afterwards Jane resigned from the company with little notice, preventing a proper hand over of her duties.

Four weeks later staff arrived at work to find that all the staff records had been deleted. When the IT staff checked the backup tapes, they found the data had been encrypted and was unusable. The total cost to the company in restoring the damaged data was \$1.2 million which did not include the cost of lost business.

Forensic analysis of the network found evidence that Jane had inserted malicious software into the network to encrypt the backups and delete the data after a set period of time. Further examination showed that Jane’s access had not been properly removed and she had been able to remotely access the network since her departure and prevent earlier detection of her actions.

- ✗ monitor staff morale
- ✗ ensure that staff access is removed quickly after they leave, and
- ✗ monitor and log any changes to the system and review those logs regularly

# INFORMATION AND COMMUNICATIONS TECHNOLOGIES

As businesses become increasingly dependent on information and communications technologies (ICT), the consequence of denial of these technologies increase.

An insider's access and knowledge of the vulnerabilities and procedures of a business' ICT may be used to cause significant damage to the business' reputation, productivity or finances.

## Access controls

Formal policies to disable access when a staff member or contractor is dismissed or leaves may reduce their ability to cause harm to an organisation.

This policy should also include any remote access that they may have as well as changing the passwords of any shared accounts that they may have used. Certificates and tokens used to access the network should be immediately revoked to prevent misuse.

## Shared administrative accounts

Shared administrative accounts should be avoided as they create a significant vulnerability to organisations.

These vulnerabilities include:

- rarely having changed passwords
- having a high level of privilege on the network, and
- causing a level of ambiguity in forensic analysis.

If a shared administrative account is required, its use should be logged, and when a staff member's role changes or they leave, the account's password should be changed to prevent misuse.

## Account management policies and procedures

In a majority of insider attacks the attacker attempts to conceal their identity. Auditing new accounts, especially those with administrative or remote access, will aid in detecting accounts used by an insider. This auditing should include verification by the account owners.

Delineating ICT roles between administrators and security personnel will increase the monitoring of systems and minimise the possibility that a malicious change will go undetected.

## Standard operating environment

The use of malicious software and scripts to delete or corrupt an organisation's data can be difficult to detect. The use of a standard operating environment (SOE) can aid in the detection of malicious software through periodically checking the current configuration of a user's environment with the SOE, and querying any changes.

## Logging and monitoring

Monitoring of system logs may allow early detection of malicious changes to the network.

System logs need to be protected to preserve their integrity, should be accessible only by security staff, and should be backed up to allow forensic analysis if there is an incident.

## Employee understanding of the consequences

The majority of insiders do not consider the consequences of their actions when undertaking an attack. Educating employees on the consequences of such attacks from both the business and perpetrator's perspective may act as a deterrent to such attacks. This includes the risk of financial losses causing retrenchments to other staff as well as criminal prosecution and jail sentences.





## MORE INFORMATION

### **Reporting Events**

In the event of an emergency – dial 000

To report possible signs of terrorism phone the  
National Security Hotline on 1800 123 400

### **Further Information**

National Security website – [www.nationalsecurity.gov.au](http://www.nationalsecurity.gov.au)

The Trusted Information Sharing Network for Critical  
Infrastructure Resilience website – [www.tisn.gov.au](http://www.tisn.gov.au)

### **Risk Management and Business Continuity Standards**

Standards Australia website – [www.standards.org.au](http://www.standards.org.au)

© Commonwealth of Australia 2010

ISBN: 978-1-921725-37-1