Australian Government

MANAGING THE INSIDER THREAT TO YOUR BUSINESS

A personnel security handbook

ISBN 978-978-1-925118-45-2

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the *It's an honour* website (www.itsanhonour.gov.au).

Contact us

Enquiries regarding the licence and any use of this document are welcome at:

Commercial and Administrative Law Branch
Attorney-General's Department
3–5 National Circuit
BARTON ACT 2600

Telephone: 02 6141 6666

copyright@ag.gov.au

Ministerial foreword

Personnel security is fundamental to good business.

Most personnel strive to conduct themselves in an ethical and professional manner. However, it would be negligent to ignore the risk of someone deliberately causing harm or exploiting their positions of trust.

The trusted insider represents a real and enduring risk to everyday business practices. It is an important risk consideration for both government and the private sector. Insider activity is, at the very least, embarrassing and damaging to an organisation's reputation, but it can also be disruptive, expensive and life-threatening.

This handbook addresses the risk of the trusted insider—a person who uses insider knowledge or access to commit a malicious act to cause harm. It provides guidance on the risks and factors associated with a trusted insider, and offers practical measures to assist organisations mitigate the threat.

A trusted insider is someone who leaks information or takes that material outside of the organisation without protecting the information appropriately or without authorisation. This is quite different from, and should not be confused with, a whistleblower disclosing information that, in the public interest, should be disclosed, as detailed in the *Public Interest Disclosure Act 2013* (Cth).

Trusted insiders represent a diversity of types and motivations. However, all have placed personal motivations and needs ahead of their obligations to their employer. Although malicious acts by insiders are rare, the potential level of risk demands that we are alert to this threat.

A number of high-profile international cases of trusted insiders have highlighted the importance of maintaining strong personnel security measures. Australia is not immune to the risk of a trusted insider and avoiding the potential level of damage from such activity requires a concerted effort.

I encourage all Australian organisations to read this handbook—not only to improve your understanding of personnel security and promote a positive protective security culture—but to help build a robust and resilient organisation.

Senator the Hon
George Brandis QC

Understanding the insider threat

Who

The insider threat can be defined as the threat posed by unauthorised access, use or disclosure of privileged information, techniques, technology, assets or premises by an individual with legitimate or indirect access, which may cause harm.

Trusted insiders are potential, current or former employees or contractors who have legitimate access to information, techniques, technology, assets or premises.

Trusted insiders can intentionally or unknowingly assist external parties in conducting activities against the organisation or can commit malicious acts for self-interest. There is no one type of trusted insider. However, there are broadly two categories of trusted insiders who pose a threat:

- **The unintentional insider:** unintentional insiders are 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 IT systems unattended and failure to secure sensitive documents, and unwitting unauthorised disclosure to a third party.
- **The malicious insider:** malicious insiders are trusted employees and contractors who deliberately and willfully breach their duty to maintain the security of privileged information, techniques, technology, assets or premises.

There are two types of malicious insiders:

- **Self-motivated insiders** are individuals whose actions are undertaken of their own volition, and not initiated as the result of any connection to, or direction by, a third party.
- **Recruited insiders** are individuals co-opted by a third party to specifically exploit their potential, current or former privileged access. This includes cultivated and recruited foreign intelligence, or their entities with malicious intent.

All **malicious insiders** intentionally use their access to resources for financial gain, or to cause harm, loss or damage. Almost all physical and electronic attacks can be assisted or conducted by an insider. Some attacks can only be committed by insiders, such as the unauthorised release of proprietary information or the sabotage of assets that only employees can access.

Most **self-motivated insiders** are the result of an individual seeing an opportunity to exploit their access while already employed, rather than having sought employment with the intention of committing an insider act.

Information obtained from an **unintentional insider** is often the result of a lack of security awareness and a failure to follow security protocols. Often, an unintentional insider acts in breach of their duty to their employer. Additionally, a trusted insider who inadvertently assists an external party may not be aware that they are allowing access to assets or passing on information, or that the resources

they are providing are valuable and wanted by someone else.

Studies indicate that most insider cases involve a self-motivated insider.[1] It is not only government employees who are targets of exploitation and recruitment as an insider; businesses may also be targeted.

What

Insider activities range from active betrayal to passive, unwitting or unwilling involvement in causing harm, including:

- unauthorised disclosure of information, including intellectual property
- physical or electronic sabotage
- facilitating third-party access to premises or systems
- corruption
- theft and fraud.

Why

There is generally no single or simple reason for an employee deliberately seeking to cause harm. Commonly, malicious trusted insiders have a number of motives for their activity. Motivations are complex and often mixed. Those who betray their organisation are often driven by a mix of personal vulnerabilities, life events and situational factors.

Key motivators for malicious insider activity include:

- financial gain
- ideology
- desire for recognition
- divided loyalties
- revenge
- adventure/thrill
- ego/self-image
- vulnerability to blackmail
- compulsive or destructive behaviour
- family problems
- negligence
- disgruntlement.

Although common motivators can be identified, they do not in isolation or in combination guarantee a person will betray their organisation.

The desire for status and peer recognition—sometimes coupled with or related to genuine or perceived workplace grievance—has been a recurring theme in trusted insider cases. Case studies indicate that financial gain was the primary motivation in 47% of trusted insider cases. However, ideology (20%), desire for recognition (14%) and divided loyalty (14%) were also common motivators.[2]

Insider activity driven by ideology and desire for recognition is often closely linked to the disclosure of sensitive information. Insider activity driven by financial gain is often linked to corruption or providing third parties with access to assets and resources.

Disgruntlement or revenge also commonly fuels insider activity. A person can become disgruntled

1 Centre for the Protection of National Infrastructure (CPNI) (United Kingdom), *CPNI Insider Data Collection Study: report of main findings*, 2013, www.cpni.gov.uk/documents/publications/2013/2013003-insider_data_collection_study.pdf.

2 CPNI 2013

and seek revenge for many reasons. Key reasons include a lack of recognition, disagreements with co-workers or managers, dissatisfaction with the job or a pending lay-off.

Studies demonstrate that 88% of insider activities were carried out by permanent staff, 7% involved contractors and 5% involved non-ongoing employees. Significantly, more males (82%) engaged in insider activity than females (18%), and 60% of the cases were individuals who had worked at the organisation for less than five years.[3]

A large number of insider acts are opportunistic (76%) rather than being the planned act of a deliberate infiltrator (6%). It is also important to note that many employees with malicious intent never commit an act of betrayal.[4]

How and when

Trusted insiders will know their employer's vulnerabilities, and how and when they can be exploited.

They will exploit their employer's trust and their access to resources and facilities to harm the business. They may abuse legitimate access or take advantage of poor access controls to gain unauthorised access.

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

Technology has exacerbated the threat from trusted insiders. Technology has broadened access to information for staff at all levels and increased the ease with which sensitive information can be aggregated, removed and disseminated.

3 CPNI 2013.
4 CPNI 2013.

Case study 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 dabble on the pokies.

In January, Melissa came back to work from Christmas holidays less motivated than normal. Word got out that she had separated from her husband. During the next few months, Melissa's demeanour and behaviour changed; she often arrived late and left early, and 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 company's chief executive officer (CEO) 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.

- Identify significant changes in an employee's personal circumstances.
- Note when an employee seems under considerable stress.
- Check whether all employees need after-hours access.
- Support and engage with the employee throughout periods of stress.

There are generally six categories of insider activity.

Fraud

Fraud can be defined as obtaining a benefit using dishonest means, or causing a loss by deception or other means. Employees or contractors may be motivated to commit fraud to gain a benefit for themselves or others, or to cause a loss to the organisation.

The dishonest benefit gained or loss caused by fraud is not just limited to a monetary cost (eg theft)—it can also encompass other resources, such as information, intellectual property and time (eg employee's fraudulently manipulating leave). The loss associated with the fraudulent act may also extend to areas such as reputational damage and risks to public safety.

Fraud can take many different forms, including:

- theft
- misappropriation
- unlawful use of property, equipment or facilities
- providing false or misleading information
- using false, forged or falsified documents.

Fraud can be committed by an individual on their own behalf or on behalf of an external agent, or by a network of individuals conspiring together. Often, fraud can be facilitated by unwitting co-workers, who are unaware they are assisting the fraudulent individual.

Corruption

Corruption can take many forms, but is typically characterised by an insider's concealed, dishonest or biased behaviour to make a profit or cause a loss.

Corrupt conduct consists of an abuse of trust, using a position or discretionary power for one's own purpose.

Corrupt practices have the potential to undermine Australia's reputation for high standards of governance, robust law and justice institutions, equitable delivery of services, and transparent and fair markets.

Some examples of corrupt conduct include bribery, embezzlement, insider trading, nepotism or cronyism, creating or exploiting a conflict of interest, and unauthorised access to or disclosure of information. Corruption can facilitate other forms of insider threat, including fraud, criminal gain and espionage.

Case study 2: Fraud and corruption

In 2013, **Joseph Hikairo Barlow** was sentenced to 14 years' jail for defrauding Queensland Health. Barlow made 65 fraudulent grant payments to himself between 2007 and 2011, totalling more than $16.6 million and including a single fraudulent payment of $11 million. Queensland's Crime and Misconduct Commission (CMC) found that, from the outset, Barlow was a high-risk employee: he had a criminal record, was wanted for questioning in New Zealand for fraud, and had fabricated his CV and his heritage as a Tahitian prince.

His conduct in the workplace manifested signs of chronic unreliability, characterised by an obvious lack of respect for the workplace, a propensity to take advantage of the service conditions, consistently poor attendance, erratic work hours that were not recorded on timesheets, excessive amounts of leave taken without proper records being kept and poor-quality work not to the standard required of his seniority level, requiring other staff to complete or redo his tasks.

Barlow would later admit that he actively intended to defraud Queensland Health. The CMC found that Queensland Health missed the initial warning signs of Barlow as a high-risk employee and failed to properly investigate when it became aware of concerns relating to his behaviour. The CMC also found that a number of co-workers assisted Barlow in carrying out his fraudulent behaviour. Although some co-workers were unwitting accomplices, the CMC found that a number failed to comply with policy and procedure, and recommended that disciplinary action should be taken against them.

- × Verify identity.
- × Check references.
- × Undertake a criminal history check.
- × Identify and manage underperformance.

Criminal gain

Private enterprise employees are attractive to organised crime because of their knowledge of business and government processes. Businesses can also give legitimacy to corrupt financial transactions and provide a cover for the movement of illicit goods, either domestically or internationally. Globally, there are many examples of trusted insiders who defraud businesses or who use a business to facilitate criminal activity, such as drug trafficking and money laundering.

Trusted insiders can be complicit in criminal activity, or may be duped or coerced into assisting criminals undertake illegal activity. They can work alone for their own personal gain or may be a small part of a sophisticated criminal enterprise. In some cases, trusted insiders have used their employment to undertake illegal activity to assist family, friends or people with a shared cultural background or beliefs.

Unintentional disclosure

A person can be unaware that they are disclosing information, or that the information they are providing is valuable or sensitive. Leaving a workstation unlocked, not securing a password or not following system procedures are examples of unintentional threats that can lead to more serious compromises. Additionally, stolen or misplaced security passes, laptops and mobile devices can also lead to unintentional disclosure of sensitive or valuable information. So too can a simple conversation about what a person is currently working on with a friend or family member.

Espionage or spying

An individual, commercial entity or government can undertake espionage (or spying) for the purpose of surreptitiously or deceptively obtaining secret information for national, commercial or economic advantage. A trusted insider can be used as a tool for either traditional espionage by a foreign government or industrial espionage.

Espionage poses an enduring threat to both the Australian Government and Australian businesses. It can provide significant unauthorised access to a wide range of information detrimental to our interests, including future prosperity.

Terrorism

Insider threat studies show that the majority of trusted insiders, who act against an organisation, do not do so for terrorist or espionage purposes, but rather for motives of disgruntlement, revenge or criminal financial gain.[5] However, trusted insiders can be extremely dangerous tools for terrorists who can leverage them to gain information or access premises.

5 CPNI 2013

Case study 3: Malicious insider

In July 2013, United States (US) soldier **Bradley Manning** was convicted of 17 charges under the US *Espionage Act* of 1917. Manning unlawfully passed classified material, including more than 250 000 diplomatic cables, to the WikiLeaks website. It is unclear exactly what motivated Manning to release the material. However, before the unauthorised disclosure of the cables, Manning displayed an ideological conflict with the war in Iraq, struggled with his homosexuality and gender identity within the US Army, and was vocal about his dissatisfaction with his work environment. Before Manning 'leaked' the cables, he had been demoted because of growing concern about his mental state and recent outbursts.

Case study 4: Espionage or malicious insider

In June 2013, **Edward Snowden**, a former Central Intelligence Agency employee and National Security Agency (NSA) contractor, illegally removed up to 1.8 million classified documents from the NSA, including material harmful to Australia. Snowden abused his privileges as an IT administrator to gain access to the majority of these documents. He also accessed a small number of documents by asking unsuspecting colleagues for their usernames and passwords.

It is estimated that Snowden shared between 50 000 and 200 000 classified documents with reporters, of which only a very small percentage have been made public so far. Even the releases to date have caused significant damage. There were a number of warning signs to suggest Snowden could become a trusted insider, including inconsistencies on his CV. He also promoted his ideological views using social media. Further reporting suggests the company that completed Snowden's security clearance is accused of signing-off on thousands of incomplete security checks.

Personnel security—what it is and why you need it

Personnel security is 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. Organisations need to have effective and robust personnel security frameworks in place.

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 (see Figure 1).

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.

The remainder of this section describes the elements of the personnel security framework in more detail.

Organisational personnel security	Make sure you: • know your business • have a good security culture • perform a personnel security risk assessment • understand the legal framework • communicate personnel security and the consequences of personnel security breaches to your employees.
Pre-employment personnel security	Perform the following pre-employment background checks: • identity checks, including overseas applicants or applicants who have spent time overseas • qualification and employment checks • national criminal history checks • financial background checks. All documents for the checks should be secured. Any applicant who fails to meet the standard of your business should be rejected for employment.
Ongoing personnel security	Make sure you: • have access controls in place • perform protective monitoring • promote a security culture, including one that - counters manipulation - reports and investigates, when necessary - performs ongoing checks - submits contractors to the same security clearance as in-house personnel • recognise after-employment threats.
Information and communications technology security	Be sure to consider and, if necessary, monitor: • electronic access • shared administrative accounts • account management policies and procedures • the standard operating environment • system logs.

Figure 1 A personnel security framework

Organisational personnel security

Know your business

You know your business best—its key roles and people, its strengths and weaknesses, and its environment and operations. When developing a personnel security framework, take into account:

- the broad operational environment
- your risk management framework
- training and education
- the key positions of trust in your organisation
- the reliability and integrity of your recruitment processes
- your human resources structure and processes
- the interaction between your human resources, and protective and electronic security areas
- the implications of incidents that result from a breach of personnel security
- the key information, technology or premises you need to protect.

Certain organisational factors in your business, or the lack of policies to address these factors, mean that there may be an increased risk of an insider threat to your business. These factors include the following:[6]

- Proprietary, valuable, classified or other protected materials are readily available or easily acquired.
- Access privileges are provided to those who do not need them.
- Proprietary or classified information is not labelled or is incorrectly labelled.
- Someone can easily exit the facility (or network system) with proprietary, valuable, classified or other protected materials.
- Policies regarding working from home on projects of a sensitive or proprietary nature are undefined.
- There is a perception that security is lax, and the consequences for theft are minimal or non-existent.
- Employees face considerable time pressures—employees who are rushed may inadequately secure proprietary or protected materials, or not fully consider the consequences of their actions.
- Employees are not trained on how to properly protect proprietary information.
- Subcultures exist within the organisation, where loyalties are to one another, rather than to the organisation itself.
- Employees have low levels of awareness of potential security and integrity risks.

Have a good security culture

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

- **Awareness:** employees understand and accept the security risks for the organisation.
- **Ownership:** security is viewed as an integral part of the organisation's business.
- **Reporting:** security breaches are reported, and employees accept reporting as normal.

6 Federal Bureau of Investigation, *The insider threat: an introduction to detecting and deterring an insider spy*, accessed 14 April 2014, www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat.

- **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.
- **Offering incentives:** ideas for improving security and reporting security breaches are rewarded appropriately.

Perform a personnel security risk assessment

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

- prioritise risks to your business
- develop a personnel security plan and identify security measures to mitigate risks
- allocate resources cost-effectively and commensurate with the risk
- help identify potential consequences or impacts
- communicate insider risks to managers and employees, and ensure that they engage with your personnel security framework.

Understand the legal framework

Understanding the legal framework is vital. When developing a 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 legislation includes that relating to:

- general discrimination, including race, gender, religion, sexual orientation, age and disability
- criminal history
- immigration status
- work health and safety
- public interest disclosure
- privacy.

Communicate personnel security to your employees

Communicating expectations within any organisation is essential to the effectiveness of its risk control measures, including personnel security. In the absence of effective communication, it can be difficult to establish and maintain an organisational culture that is resistant to insider threat. The following factors are important to this process:

- The head of the organisation and senior management visibly demonstrate their commitment to security and integrity (often referred to as 'tone from the top').
- Managers and supervisors play an active role, and are:
  - close enough to employees and processes to identify risks and problematic behaviour

- able to exercise direct control over these risks and behaviours
- able to maintain an awareness of the organisational value of security and integrity.

- Employee and organisational values are aligned, including through raising awareness of ethical behaviour.
- Staff confidence in the available reporting mechanisms is fostered, both in terms of protection for the reporter and subsequent fair treatment of the subject of the report.
- Minor misconduct is addressed diligently and fairly—this prevents a misconduct-tolerant environment from forming, which can lead to more serious breaches.

Pre-employment personnel security

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.

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 the recruitment process, advise all applicants about:

- the business's requirements for pre-employment checking
- why these checks are conducted
- what your business will do with the information collected
- to whom the information might be disclosed
- what subsequent decisions might be made about an applicant's 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.

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 the Australian Standard AS 48112006 (Employment screening) and the Standards Australia publication HB 323-2007 (Employment screening handbook).

These publications can be found at 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 (as far as possible) to conduct the same checks as for applicants who have 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

When confirming an applicant's qualifications, you should:

- request original certificates or copies certified by the issuing authority
- compare details in these certificates with those provided by the applicant
- confirm the existence of the educational institution and the details provided by the applicant.

You should check the details in an applicant's curriculum vitae (CV) to ensure that there are no unexplained gaps or anomalies. Where possible, you could 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.

Case study 5

Peter, 49, 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 that had made a lot of money quickly. The chief executive officer (CEO) was an ideas man and trusted Peter to look after the money side of things. Ten months after Peter took over as chief financial officer, regulations changed and five new businesses entered the market. Peter informed the CEO and executive that, although the company was still profitable, profits were likely to be less than forecasted. 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, and the remaining 110 were told that their future was shaky. A consulting accountant quickly found that Peter had stolen nearly $2 million from the company and had hung on until the very last minute before it all came crashing down. The matter was referred to the police.

Peter could not be tracked down. Police soon found that he had given a false name to the company when he was recruited, and that 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.
- Note significant unexplained changes in an employee's circumstances.

National criminal history checks

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 convictions scheme. You should also bear in mind that, just as a criminal conviction is not necessarily a barrier to employment, a clean record does not 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 might consider conducting a financial background check or requesting 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

For any pre-employment check, you should ensure that all documents are securely held and made available only to those who can demonstrate a need to access the information.

Procedural fairness

If an applicant fails to meet the standards that your business (and/or legislation) has set and their application for employment 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. They can 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 to access certain material. You should issue passes from a single location or section to reduce the possibility of duplication or confusion.

Protective monitoring

Your physical access control system should enable you to monitor any breaches or attempted breaches.

For particularly sensitive areas, you could use a system that provides real-time alerts of unauthorised access. You could also 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 it is that you will identify unusual behaviour. Layering increases cost and needs to be based on the risks identified.

Security culture

Countering manipulation

Individual insider activities can be difficult to predict or detect. However, there may be signs that an employee is vulnerable to becoming an insider.

Studies reveal a number of indicators to watch for. It is important to note that these are signs of general stress and do not necessarily indicate a propensity to become an insider. They include:

- 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

Tips for improving security

- ✓ Where pass or swipe cards are used, beware of individuals tailgating others to gain access to areas of interest.
- ✓ Limit access to files, documents, systems and physical locations to only the individual employees who need this access to undertake their work.
- ✓ Review the need for individuals who have not undergone appropriate screening to enter or access sensitive areas. Escort or monitor contractors, visitors and other non-employees.
- ✓ Develop ongoing employee awareness, assistance and screening programs.
- ✓ Consider obtaining legally binding confidentiality undertakings from staff working on potentially sensitive projects.
- ✓ Alert staff to the potential threat of corporate or state-based espionage when they are travelling overseas. Develop a system of reporting when employees return from overseas travel and believe that they might have been a target of espionage.
- ✓ In highly sensitive areas, consider restricting the use of electronic devices such as mobile phones, cameras and thumb drives.
- ✓ Consider limiting the use of social media websites in the workplace, and of discussing work-related issues on social media websites.
- ✓ Encourage employees to report suspicious behaviour, contacts, enquiries and security breaches.

- creditors calling at work
- sudden and unexplained wealth
- inappropriate interest in sensitive or classified information
- accessing (or attempting to access) restricted areas or information outside an employee's realm of responsibility
- taking video, photos, diagrams or notes of restricted information
- working unusual hours
- unexplained absences or travel
- repeated breaches of organisational security requirements
- unexplained or concealed contact with foreign nationals
- refusal to take leave, or only taking small amounts to prevent others from acting in their position
- taking possessive control over certain aspects of work
- unusual interest in choosing new staff
- giving unusual gifts to other colleagues.

If an individual demonstrates one or two of the traits above, this does not necessarily mean that they are an insider threat. However, if an individual is demonstrating a combination of these traits, it should trigger an investigation into the individual.

Your employees should be educated to recognise the signs of insider behaviour. They also need to be aware that the following behaviour could indicate that someone from outside the organisation is attempting to gain privileged access or information:

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

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

Reporting and investigation

Suspected breaches of 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 maintain confidence in your personnel security measures.

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

- **Guidelines:** establish guidelines (if they do not already exist) for running an investigation, including when matters should be investigated, when matters should be referred or outside assistance sought, how evidence will be gathered, how witnesses will be approached, who will run the investigation and how the outcome will be determined.
- **Benefit of the doubt:** in many cases, there may be a simple explanation for a security breach, so, if possible, give the employee the opportunity to explain. If this is not possible, consider when to inform the employee that 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.
- **Morale:** be aware that an investigation, even one handled well, can have an adverse impact on employees.

Case study 6

George, 24, worked for a large company in the resources sector. He came from Europe and had been in Australia for six months. 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 that their supervisor treated George's talk with derision.

One morning, George's colleagues arrived at work to find that the company's equipment had been spray painted, its tyres slashed and its 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 that the company cease operations immediately and give 80 per cent of the past year's profits to charity. He said the company was committing environmental terrorism.

After hours of negotiation the police removed George and his friends. Although they discovered that the bombs were crude hoaxes, the company lost more than $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 employees with 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 they are concerned about these views and express their concerns to other managers.
- ✗ Check whether all employees need after-hours access.

Ongoing checks

Consider whether you would like to repeat any of the pre-employment checking stages when an employee applies for a promotion or at regular intervals during the person's employment.

Contractors

Although contractors pose additional challenges, they should be included in your personnel security framework to the greatest extent possible.

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

If you use identity or access control passes, it is a good idea to have a specific identifier to indicate a contractor. Once the contract has finished, it is very important to ensure that the contractor's access cards are deactivated and the contractor returns all access cards.

After employment

Recognise that ex-employees may still pose a threat and observe the following precautions:

- Ensure that access of former employees and contractors to physical facilities, and to information and communications technology (ICT) systems is revoked immediately after they depart.
- Set clear boundaries and rules for ongoing professional networking between present and former employees.
- Undertake exit interviews of departing staff. Interviews should include an opportunity for staff to confidentially express any security concerns relating to procedures or colleagues.

Businesses should ensure that their work environment limits the potential for the integrity, availability and confidentiality of sensitive information to be compromised. Balance the 'need to know' against the 'need to share'. Suitable measures need to be carefully considered, implemented and tested regularly for their effectiveness.

Information and communications technology security

As businesses become increasingly dependent on ICT, the consequences of being denied access to these technologies also increase.

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

Organisations need well-structured systems that protect the business' 'crown jewels'.

Electronic access

Organisations need to have well-structured ICT systems that allow necessary access for personnel to undertake their work, but protects their key information, technology and intellectual property.

Organisations should implement robust ICT systems. ICT systems need to be regularly reviewed, auditable and well structured to ensure that key corporate information is protected and only accessible by those with a genuine need to know.

Case study 7

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

During a corporate restructure, Jane's role was changed. Jane voiced 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 handover 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 that the data had been encrypted and were unusable. It cost the company $1.2 million to restore the damaged data, not including the cost of lost business.

Forensic analysis 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 after her departure and prevent earlier detection of her actions.

- Monitor staff morale.
- Ensure that staff access is removed quickly after they leave.
- Monitor and log any changes to the system, and review the logs regularly.

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.

These policies should include removing any remote access that an employee has been given, as well as changing the passwords of any shared accounts that they 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 because they are a significant vulnerability for organisations.

These vulnerabilities may include:

- passwords that are rarely changed
- access to a high level of privilege on the network.

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

Account management policies and procedures

In most 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—that is, the current configuration of a user's environment can be periodically checked with the SOE, and any changes queried.

System logs

Monitoring system logs may help you to detect malicious changes to the network earlier.

System logs need to be protected to preserve their integrity—only security staff should have access to them, and they should be backed up to allow forensic analysis if there is an incident.

Conclusion

The majority of insiders do not consider the consequences of their actions when undertaking an attack. Educating employees about the consequences of such attacks from the perspective of both the business and the perpetrator may act as a deterrent to such attacks. Consequences include the risk of financial losses, leading to retrenchment of staff, as well as criminal prosecution and jail sentences.

Further information

Reporting events

Reporting a crime to the Australian Federal Police: www.afp.gov.au/contact/report-a-crime

Reporting possible signs of terrorism: National Security Hotline (1800 1234 00)

General information

National security: www.nationalsecurity.gov.au

Protective Security Policy Framework: www.protectivesecurity.gov.au

Fraud: www.ag.gov.au/fraud

Anti-corruption: www.ag.gov.au/CrimeAndCorruption/AntiCorruption

Trusted Information Sharing Network for Critical Infrastructure Resilience: www.tisn.gov.au

Australian Security Intelligence Organisation Business Liaison Unit: www.blu.asio.gov.au

Risk management and business continuity standards

Standards Australia: www.standards.org.au

Bibliography

Centre for Protection of National Infrastructure, *CPNI Insider Data Collection Study: report of main findings*, 2013, www.cpni.gov.uk/documents/publications/2013/2013003-insider_data_collection_study.pdf.

Federal Bureau of Investigation, *The insider threat: an introduction to detecting and deterring an insider spy*, accessed on 14 April 2014, www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat.