It happens here

Managing the insider threat to your organisation

PSR | Protective Security Requirements

Contents

Introduction

Unless you work in the security field, you probably haven't spent much time thinking about 'insider threat' — the potential for people you work with to harm your organisation. Even if you have considered the risks, you might think your organisation is safe, or that if something happens, it won't be too bad.

In reality, many New Zealand organisations have failed to protect themselves from insider threat, and been badly damaged as a result. They've struggled to recover from financial losses and reputational hits, not to mention the impact on morale after someone betrays everyone's trust.

If you're complacent and think 'it won't happen here', your organisation won't be as prepared or protected as it should be.

The good news is that you can learn to recognise the signs of insider threat, and how to prevent insider threats from escalating.

We can all play a role in creating a security culture that protects our organisations, our people, and the work we do. It all starts by remembering 'it does happen here'.

About this guide

The New Zealand Intelligence Community (NZIC) has developed this guide to support your organisation so you can:

- recognise and manage potential insider threats
- improve your people's security behaviour (your security culture).

Apply the advice in this guide to all current and former employees and contractors, regardless of whether they hold a national security clearance or not.

Use our advice to raise awareness that 'it does happen here' and break through the barriers to good security.

Note: The case studies we've included in this guide are inspired by real events. However, people's names and many of the details are fictitious.

Every organisation is vulnerable to insider threats from its employees.

In New Zealand, the most common types of insider acts are theft, fraud, corruption, and poor security behaviour.

PSR: Protective Security Requirements

What is insider threat?

'Insider threat' describes the potential for people to use their authorised access to your organisation's work locations, people, information, and systems to cause harm.

When you consider insider threats, think about:

1. People you're hiring
2. Current and former employees
3. Current or former contractors.

Insider threats or acts can take many different forms and cause harm in various ways.

INSIDER THREAT:	EXAMPLE OF HARM:
Theft, fraud, and corruption	Financial losses
Information leaks	Reputational damage, loss of intellectual property
Privacy breaches	Compromised customer or client information
Sabotaged systems or equipment	Disruption to operations
Violent acts or threats	Safety and wellbeing at risk

The threat of harm to your organisation is greatest when someone working for your organisation:

- misuses their authorised access
- is granted access outside their area of responsibility
- shares sensitive or valuable information inappropriately
- misuses or steals resources
- behaves in a threatening manner.

People working for your organisation can also cause harm through human error or poor security behaviour. For example, they could accidentally email the wrong people, click a link in a phishing email, or talk about work matters while on public transport.

Types of insiders: intentional and unintentional

Insiders who cause harm fall into two broad groups — those who act intentionally and those who act unintentionally.

Intentional insiders

'Intentional insiders' aim to cause harm. They're either recruited by an external party or self-motivated.

An intentional insider who is recruited usually responds to external pressure. That pressure could come from people who share their ideology, or an external party with leverage over them. For example, a gang could apply pressure to repay a debt, or a representative of a foreign government could apply pressure to get access to information.

An intentional insider who is self-motivated is usually motivated by ideology, or driven by financial gain. Possible influences on their behaviour are:

- financial difficulties
- greed
- wanting to be perceived as wealthy
- being deeply opposed to a decision or stance your organisation has taken.

> *When security awareness is low, employees tend to think security is not important. This attitude is especially likely in New Zealand because we tend to minimise the risk of security threats — and sometimes bad things in general — with 'it won't happen here'.*

Unintentional insiders

'Unintentional insiders' cause harm accidentally and the most likely cause is poor security behaviour.

An unintentional insider might not know the correct security processes, might ignore security processes (thinking they are irrelevant), or might bypass them because they're in a hurry. Other factors such as stress, high workload, and poor communication can also be behind some unintentional insider acts.

Poor security awareness could mean an employee:

- has a genuine gap in their knowledge about the security behaviour expected of them
- hasn't paid attention to induction materials or other training about security
- doesn't understand the potential impacts of not following security processes.

CASE STUDY 1

Long-serving, trusted manager accepts bribes

Angela joined a large public service organisation when she was 20. By the age of 45, she was a national manager responsible for contracts worth millions of dollars.

Angela was a highly valued and trusted member of the management team. Her long stint in the organisation meant she had a broad range of institutional knowledge and access to privileged information.

Valuable government information is passed to a business associate

During the bidding process for a valuable contract, Angela became aware that a company she'd had previous dealings with was planning to put in a bid. She was friendly with one of the directors of the company — Sarah. While socialising, they came up with a plan to help the company win the bid. Angela agreed to accept a large amount of cash and an overseas trip if the bid was successful. In return, she gave Sarah inside information to help her company get the contract.

The secret deal was successful. The inside information was crucial to the company winning the bid. Angela pocketed the money and took the trip, even excitedly telling her team about her travel plans before she left.

Changes in behaviour raise suspicions

What Angela didn't know was that her behaviour had raised suspicions. She had been quite guarded about this particular contract. So much so that members of her team felt something wasn't right. They began to talk and share information. One team member had overheard Angela speaking to Sarah on the phone in a very friendly manner, and started to wonder if there might be a conflict of interest.

Luckily, some of the team members took their concerns to the HR manager. The ensuing investigation resulted in Angela being found guilty of corruption and bribery by the Serious Fraud Office. Sarah was found guilty of fraud.

- Don't assume a long-serving employee won't commit an insider act
- Watch out for changes in behaviour
- Ensure you have secure processes in place
- Check for conflicts of interest

PSR: Protective Security Requirements

What to watch for

Security intelligence communities around the world recommend you make everyone in your organisation aware of the following common signs of insider threat. Remember that the presence of any of these common signs doesn't automatically mean you have an insider threat. However, you should tell your security team what you've noticed.

Changes in behaviour / Significant life changes

- Being more nervous and anxious than normal
- Receiving calls from outside work that cause stress
- Becoming wealthy suddenly without any explanation

Concerning or unusual behaviour

- Being under the influence of drugs or alcohol
- Making extreme statements that show bitterness or anger — especially towards your organisation and its work, or more senior colleagues
- Not wanting to take leave and being nervous about others acting in their position — being possessive about certain pieces of work
- Having an unusual interest in choosing new employees

Changes in work performance or habits

- Poor work performance
- Unusual working hours — especially repeated after-hours access
- Unexplained absences or travel

Security violations

- Breaching security processes repeatedly, or deliberately not following security policies
- Asking others to overlook security breaches, such as not wearing an ID tag or carrying a security pass

Attempts to access sensitive information or restricted areas

- Being more interested than normal in sensitive information (especially information they wouldn't usually have access to)
- Attempting to access (or successfully accessing) restricted areas that are outside their normal responsibility
- Taking videos, photos or notes/diagrams around sensitive information

CASE STUDY 2

Draft policy leaked to a political party

Derek felt strongly opposed to a policy being developed in the government organisation he worked for. It went against many principles he held dear. The more he heard about the policy, the more annoyed and concerned he became.

Derek had heated debates with people in the policy team. He was known to be passionate about his views, so no one was too concerned when he disagreed with the policy. They trusted him to be professional when it counted. Derek was also generally well liked and played social football alongside members of the policy team.

Temptation leads to action

When Derek noticed pages from the policy sitting in the printing tray, temptation overcame him and he took them. He planned to use what he learnt to persuade members of the policy team that the policy was flawed.

Later that night, he was chatting online with a group of people opposed to the same things as him. He got fired up and started to focus on another idea. What if he leaked the draft policy? If it ended up in the media, the publicity and controversy could make the policy impossible to implement.

Derek made up his mind to leak the policy to a politician known to oppose the policy's underlying principles. The resulting media attention and public reaction was so intense that the policy was put on hold.

Hard work goes to waste

Meanwhile, speculation about who leaked the policy was rampant at Derek's workplace. Privately, a few people suspected him, but they didn't say anything. They didn't have any proof, did they? And he was a good guy, wasn't he? No one wanted to point the finger, so the whole policy team endured being under suspicion and seeing all their hard work quietly shelved.

With only suspicion and no proof, Derek suffered no consequences and nothing would prevent him leaking information again if the opportunity arose.

- Watch for expressions of anger against your organisation
- Check that you haven't left any pages in the printing tray
- Report concerns or suspicions to your security team — they know what to do, and how to keep information secure

Why do people do it?

Although financial gain is the most common reason for an insider turning against their organisation, there's often a combination of reasons at play.

The following list gives the most common reasons for insider acts. Remember that there may be other reasons — the presence of a common reason doesn't automatically mean you have an insider threat.

Being disgruntled or angry

- Outwardly displaying signs of anger or resentment with their employer, manager, or colleagues
- Seeking revenge against their employer, manager, colleagues, or someone they know

Seeking recognition, admiration, or thrills

- Having a desire for recognition (notoriety)
- Attempting to boost their self-esteem or image
- Thrill-seeking, risk-taking

Having relationship or personal problems

- Having relationship problems with family, friends, or a partner
- Having health or personal issues that cause compulsive or destructive behaviour

Being influenced by others or an ideology

- Having divided loyalties or a conflict of interest (for example, between their employer and someone they have a personal or work relationship with)
- Believing in or developing a belief in an ideology or cause (especially one that opposes their employer and its work)
- Succumbing to external pressure, such as blackmail or pressure to repay a debt

Not caring about security

- Not following security processes despite knowing them
- Failing to act when a security concern is raised

Financial gain is the single most common motivation for an intentional insider act.

Source: CPNI Insider Data Collection Study 2013

PSR: Protective Security Requirements

CASE STUDY 3

Security bypassed to get a contractor started quickly

A prominent public sector organisation running a large infrastructure project experienced multiple security breaches and costly delays due to a manager's poor security behaviour.

This manager was motivated to bypass correct security practice — including completing the paperwork to allow a contractor to access the organisation's systems — to bring a contractor on quickly so that project deadlines could be met.

Skipped paperwork results in multiple security breaches

- The contractor did not have their own ID or access card for the building. Instead, they tailgated until a temporary card was issued, and simply never returned it.
- The contractor did not have access to the organisation's systems, so others in the manager's team emailed work files to the contractor's personal email address.
- The contractor did not have one of the organisation's devices, so used their own laptop.

Because the paperwork wasn't done, sensitive project information was put at risk of disclosure and the security team couldn't put the usual measures in place to protect its information, systems, resources, and people.

Not following the correct process creates a costly delay

When the head of security discovered these security breaches, the contractor was stood down until their access could be approved. The stand-down period caused the project team to miss their first big milestone and cost-overruns became inevitable.

When the manager was asked why they didn't follow the correct security processes, 'I was too busy' was the reply. The manager lost standing in the organisation and their chance to manage other high-profile projects.

While the pressure to deliver is real and common across all organisations, the consequences of bypassing security processes are not worth the risks.

- Always comply with your organisation's access protocols
- Ensure contractors are treated the same as other employees
- Allow time for orientation and on-boarding in your work plans

Factors that could lead to a insider threat

It's helpful to know the potential pathway to someone committing an insider act. The critical path model shows you the main stages and indicators to watch out for.

When personal predispositions combine with external stressors, they can compound over time and result in concerning behaviour. If the organisation involved doesn't address the behaviour, or aggravates it, the person may end up committing an insider act.

Remember that the indicators in the model are not in themselves evidence of an insider threat. Instead, they help us to know when we need to pay more attention to certain predispositions, stressors, or concerning behaviours.[1] It may also be valuable to include other factors that may impact a person, such as economic or political factors.

When an organisation, or someone in it, knows about concerning behaviour but doesn't take the right action, they could increase the likelihood of an insider act occurring.

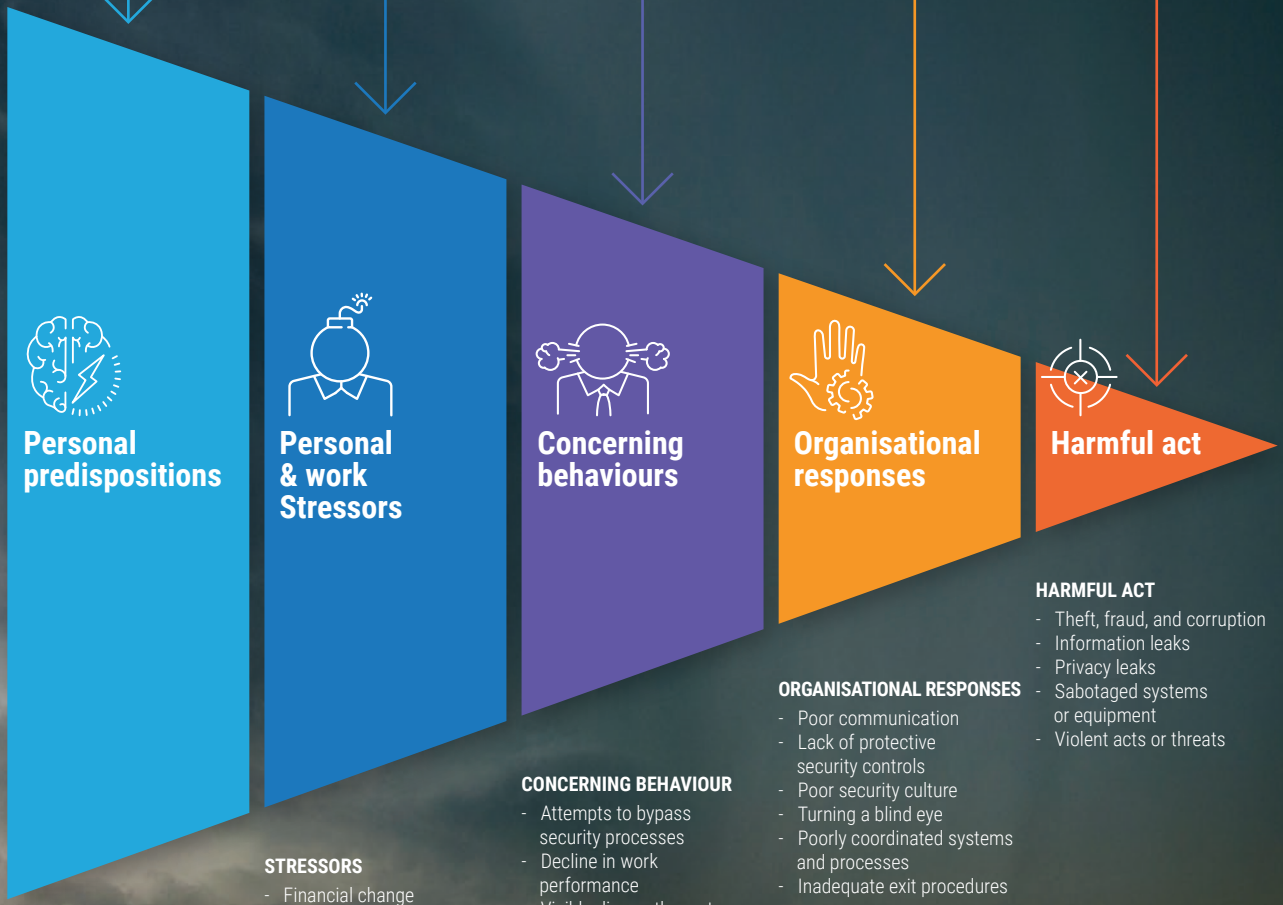
The most common cause of not taking the right action is a poor organisational response. In turn, the most common causes of a poor organisational response are a poor security culture, a lack of security measures, and poor communication.

[1] *Text adapted from educational resources belonging to the New Zealand Defence Force.*

Environmental context

Social / Economic / Political / Cultural / Organisational

Critical pathway



PREDISPOSITIONS

- Medical/psychological condition
- Personality or social skill issues
- Amoral and unethical
- Immature
- Manipulative

STRESSORS

- Financial change
- Family problems
- Job restructures
- Health problems
- Grief

CONCERNING BEHAVIOUR

- Attempts to bypass security processes
- Decline in work performance
- Visible disgruntlement towards employer or co-workers
- Drug and alcohol abuse
- Criminal behaviour
- Poor judgement and decision-making

ORGANISATIONAL RESPONSES

- Poor communication
- Lack of protective security controls
- Poor security culture
- Turning a blind eye
- Poorly coordinated systems and processes
- Inadequate exit procedures

HARMFUL ACT

- Theft, fraud, and corruption
- Information leaks
- Privacy leaks
- Sabotaged systems or equipment
- Violent acts or threats

Source: Adapted from Studies in Intelligence Vol 59, No. 2 (Extracts, June 2015), Shaw & Sellers

How do you protect yourselves?

Adopting the Protective Security Requirements (PSR) is your organisation's best protection against the insider threat.

The PSR outlines the government's expectations for security governance and for personnel, information, and physical security. In the PSR, you'll find advice on how to meet these security expectations, including how your organisation can reduce the risks and impacts of insider threats.

In New Zealand, some public sector organisations must adopt the PSR, while others are encouraged to adopt it as good practice. Businesses can also benefit from adopting the PSR. You can find the PSR at: *protectivesecurity.govt.nz*

Build a good security culture

Being aware of the four major barriers to a strong security culture is a good start.

These barriers are:

1. The belief that day-to-day job pressures make people **too busy** to follow best-practice security behaviours.
2. The perception that there's **no real danger** from insider threat and the harm it can cause.
3. The thought that **'none of my colleagues are capable of committing insider acts'**.
4. The belief that it's **against Kiwi culture to dob in a colleague** we suspect of committing insider acts.

These barriers won't be overcome easily, but there's still plenty we can all do to foster a strong security culture, or further improve the one we have.

Security is everyone's responsibility. Building a strong security culture means getting everyone on board.

Senior management

Fully committed to security policies and procedures. Encourage a loyal, committed workforce.

Line managers

Often first to notice unusual behaviour. Support vulnerable and disaffected employees. Can intervene to prevent problems becoming serious.

Employees

Fully aware of security responsibilities. Receive security induction and refresher training. Can access confidential reporting system.

1.

Set expectations

Do thorough pre-employment checks

Your organisation must carry out pre-employment checks on everyone you're considering employing, including people changing roles, contractors, and short-term employees. Do not skip pre-employment checks because of a person's background, work experience, or seniority.

At a minimum, you should:

- confirm the person's identity, nationality, and right to work in New Zealand
- check the person's references with their former employer
- conduct a criminal record check.

For roles with a higher risk profile, consider doing extra checks such as psychometric testing, a credit check, qualification checks, or Police vetting (a criminal history check).

> *Don't skip or rush pre-employment checks for any potential employee, including contractors.*

Collaboration is key: security, HR, and procurement teams should work together to set policy and communicate it to managers who make hiring decisions.

Set good security expectations at the start

To set your security expectations from the start, make security education part of your organisation's induction programme. Introduce new people to your security policies and processes, and help them understand why they're important.

2.

Raise awareness and plan

Raise awareness of the common signs of insider threat

Everyone who works for your organisation needs to know how to spot the common signs of insider threat — either before they happen or once insider acts are under way.

Good communication about security is a core part of awareness, but many other parts of an organisation have a role to play, including legal, HR, security, and the executive leadership team.

> *Collaborating on awareness campaigns is the most effective way of embedding good security awareness.*

Have a plan for dealing with insider threats

Knowing how insider threats will be dealt with is very important. Just as raising awareness is best if it's collaborative, so too is planning for a breach.

Because insider acts can cause serious reputational damage, effective planning is required. Coordination between managers (with support from their executive team), and between security, legal, HR, and communications teams is important.

A breach from an insider act may require a crisis response. The response will only be effective if there are clear lines of responsibility and those rolling out the plan know in advance exactly how it should unfold.

> *Because insider acts can cause serious reputational damage, effective planning requires coordination.*

3.

Monitor, report, and reward

Monitor access to your information and systems

Line managers and security teams need to work together to ensure that information and systems are only accessed by authorised people. You'll also need to monitor regularly to pick up any unauthorised access or misuse of information or systems.

Have reporting mechanisms in place

Encourage everyone to report security breaches or near misses, and tell someone when they have concerns (someone in your security team or a manager).

If anyone feels uncomfortable about reporting, remind them they are acting in the best interests of their organisation and everyone in it, including themselves.

Reward reporting of security issues

Reward people who report security issues to help make reporting 'the way your organisation does things'.

If anyone becomes aware that an employee may harm others or their organisation, they must report it. The Privacy Act does not stop people sharing this kind of information.

4.

Act and educate

Act quickly when a breach or concern is reported

Make sure you have policies and processes in place to help you respond to security reports. Follow up quickly to prevent further harm. Once the threat has passed, adjust or improve your processes to prevent future problems.

Provide ongoing security education

Go beyond induction training and give your people ongoing support to understand what is expected of them — what good security behaviour looks like.

Some organisations run security awareness campaigns to encourage their people to call out poor security behaviour, or to make sure everyone knows what the right security behaviour looks like.

Act on poor security behaviour

After a security breach, be proactive and give the person support and training before their behaviour becomes a more serious concern.

When someone repeatedly breaches security or deliberately flouts your security measures, work with their line manager to address the concerning behaviour. You might need to put extra security measures in place or use a risk management plan to address the behaviour.

5.

Support and manage

Support people through stressful times

Stress is a big contributor to both intentional and unintentional insider acts. Look after people affected by personal or workplace stress. Big life events or work restructures can be especially stressful times.

Proactively offer or remind people about your wellbeing assistance programmes. Aim for a culture where people feel they can share issues before they worsen, so that you have a chance to provide support.

Manage departing employees effectively

In many roles, employees give their manager four weeks' notice of their intention to resign. That's a lot of time for someone to carry out an intentional insider act, or to relax so much that an unintentional breach happens. Managers need to stay vigilant during this period.

> *After someone resigns, stay vigilant and manage their departure to minimise risks.*

Ideas for raising awareness of the right security behaviours

- Offer rewards for doing the right thing
- Create activities or games that educate people in a fun way
- Publish tips that help people know what to do
- Create a short presentation for your executive team — focus on your top three insider threats and how they could impact your organisation
- Plant 'mystery shoppers' to find out if your security measures are being followed. Reward people who are doing the right things, and educate those who are not

PSR: Protective Security Requirements

CASE STUDY 4

Stress response leads to serious security breach

Gary was a system engineer for a government organisation that deployed people into volatile situations overseas. While his role was to support operations, he worked in a tense atmosphere — the danger of conflict erupting in the area was ever present.

A workmate was kidnapped and held for ransom. Several shootings took place close to where he was working. His accommodation never felt completely safe and he slept poorly most nights.

Gary began using drugs to help deal with the stress and anxiety. He could sleep better and function properly at work. When he tried to go without them, he felt ill and very nervous. Pretty soon, he couldn't go a day without the drugs.

Opportunities to detect drug use are missed

When his deployment ended, Gary returned to work in New Zealand. He didn't tell anyone how stressful his deployment was. His debrief was cursory, mainly checking that he'd followed processes and returned equipment.

His next assignment was with a different team, who knew nothing of his overseas deployment or the stress he'd been under. Because Gary was a trusted employee who'd worked with highly classified information, his new team manager skipped the normal pre-employment checks, including drug and alcohol testing.

Sensitive information is sold to fuel a habit

Fast running out of money for his drug habit, Gary used his national security clearance to steal classified information about the overseas operation he'd been part of. He sold the information to a foreign intelligence agent who'd approached him while he was deployed.

Gary's stress response led to uncharacteristic behaviour. By the time his offending came to light, he was highly addicted and his actions had put his former workmates in grave danger.

- Give wellbeing assistance to employees working in stressful environments
- Conduct thorough debriefs
- Do not skip pre-employment checks because someone is known

The big five: simple security behaviours

Encourage the following simple security behaviours to help your organisation reduce the threats from both intentional and unintentional insiders.

1.

Watch out for tailgaters

In restricted access buildings where you need a swipe card to get in, watch out for tailgaters — people following you in lifts or through restricted access doors.

Don't use your card to allow other people access, no matter how nicely they ask, how senior they are, or how closely you work with them.

2.

Question people who aren't wearing ID

If someone should be wearing ID and they are not, ask them where their ID card is. Simply say, 'Hey, where's your ID card?' or 'Excuse me, do you have your ID card?'

If questioning someone is difficult for you or the person concerned is senior to you, tell your security team what you saw.

3.

Lock your devices

Lock your devices when you get up from your desk or have finished using them — even if you'll only be away a few minutes. This simple practice prevents unauthorised access to information and systems.

PC – Ctrl + Alt + Del (or Windows + L)
Apple – Command + Control + Q

You should also take extra care when you're out and about to prevent people from seeing what you're reading or viewing on a device.

4.

Protect documents

Collect your printing as soon as it's done, don't leave it sitting in the paper tray for anyone to grab. If the content is protectively marked, use your organisation's secure printing method.

Lock documents away in drawers or cabinets and operate a clear-desk policy (keep work-related information out of view).

When you're travelling for work, follow your organisation's security policy for protecting any documents you'll have with you.

5.

Speak up

If you notice something concerning, speak up. Tell your manager or someone in your security team straight away.

New Zealand Government