COUNTER FRAUD CENTRE
Tauārai Hara Tāware

Introduction to Insider Threat

APRIL 2023

Table of Contents

1 Introduction

An insider threat is someone who can cause harm to an organisation from within. Anyone who has authorised access to an organisation's information, systems or people, including employees, contractors, vendors or business partners, can be classed as an insider threat.

This guide seeks to raise awareness of the risks posed by insider threat in the New Zealand public sector. First, we will introduce the concept of an insider threat, followed by some of the motivating factors that might drive people to carry out an attack against their organisation. Section four outlines some red flags to look out for, and the final section offers practical tips organisations can use to help mitigate the risk of insider threat.

1.1 Stay alert to the risk

As public servants we act with a spirit of service to the community and meet high standards of integrity and conduct in everything we do. Trust and confidence in the New Zealand public sector rank among the highest in the world. While most fraud risk to the public sector comes from external sources, occasionally someone may be enticed through pressure or opportunity to use an organisation's assets for their own personal gain. It is up to us all to know how to identify and be alert to insider threats.

In New Zealand the most common risk of insider threat are fraud, theft of intellectual property, and corruption. A breach of trust within an organisation may also take the form of information leaks, privacy breaches or sabotaged systems. Agencies should recognise if the information they hold might be valuable to others and ensure that there are security controls in place to protect it.

Much as organisations are alert to risk across all parts of the business, including health and safety, financial and environmental risks, they should also be alert to the risk of insider threat. A general lack of awareness can heighten the risk of insider threat. It can help if employees are able to identify and report red flags in others' behaviours.

1.2 Protect your most valuable asset – people

People are what make the public sector tick, but they can also be a source of weakness. Organisations should seek to protect their employees from harm but also from harm being caused to the organisation, whether inadvertently or deliberately. This can be achieved by fostering a strong ethical culture within an organisation. Supporting the health and mental wellbeing of all employees will help them withstand pressure or opportunity. It is the responsibility of all employees to contribute to an ethical workplace culture and this includes speaking up where appropriate. Organisations should provide avenues to report suspicious behaviour anonymously.

If a public sector employee misuses their access to information, decision making processes or assets there may be consequences for the individual, the public, or even the government. An employee may have knowledge of weaknesses within an organisation, and how they can be taken advantage of. The employee could be at any level of the organisation. Even the longest-serving employees could be involved.

When an employee knows about concerning behaviour but does not act appropriately on it, this could increase the likelihood of a breach of trust. If a breach has happened accidentally, it may be that an employee needs more support and training to ensure that it does not happen again, or there may be improvements that could be made to the system.

Organisations should encourage everyone to report security breaches or suspicious behaviours, even near misses, and tell someone when they have any concerns. If repeated security breaches are happening, no matter how minor, an organisation should respond quickly and follow organisational response policies and processes.

There are some proactive measures that agencies can take to ensure the safety of the organisations, such as:

- Creating a culture of ethical behaviour
- Teaching employees that with access comes responsibility
- Raising awareness of the common red flags
- Encouraging people to speak up if they see something that doesn't seem right.

For information on fostering an ethical organisational culture see the Office of the Auditor General's Integrity Framework.

1.3 Fraudsters don't discriminate

Fraud risks may come from any level of an organisation. A range of motivations could make a person susceptible to becoming a malicious insider. Many people believe that their colleagues are incapable of acting maliciously against the organisation they work for. That's because most of us work hard and with integrity every day.

It pays to remember that there are employees all across an organisation who may have access to sensitive or valuable information and may sometimes see an opportunity to share that information or to make a decision that benefits themselves.

Even if information does not seem valuable to the employee, external parties may be able to use it to their benefit. They could offer a financial incentive to those who have access to it.

The impacts of fraud and corruption can negatively affect the lives of all citizens. Some examples of the impact that fraud and corruption might have are:

- limiting access to public health services,
- by-passing environmental or health safeguards,
- reducing access to education, or
- enabling criminal activity.

The impact on services could be wide ranging and involve financial loss, or disruption of organisations and services. Fraud also creates a threat to democracy and the trust that people have in the government. Vulnerability to insider threat can take many different forms.

2 Types of insiders and vulnerabilities

There are two different types of insiders – those who act intentionally to harm an organisation or those who act unintentionally. It is often difficult to determine whether an employee is simply doing their job or is working maliciously.

An insider may use stealth or deceit along with their personal knowledge, to access restricted information or make unauthorised decisions.

If they act to harm an organisation, insiders can cause more damage than can outsiders. Insiders are more familiar with security networks and with the vulnerabilities of the organisation, and can abuse the trust the organisation has in them.

An insider has the advantage of being able to:

- operate at the margins of normal business practices,
- establish new behavioural patterns,
- change operational procedures to avoid detection, and
- exploit the trust the organisation has in them.

2.1 Types of insiders

Unintentional or accidental insiders

Unintentional insider threat cause harm due to negligence or without malicious intent. An employee might intentionally bypass security processes that they do not believe to be important, or if they have a genuine gap in their knowledge about behaviours expected of them.

A lack of training or poor communication around what is and is not allowed by an employee in their specific role may mean staff unwittingly access information they were not meant to. An accidental breach can still have wide reaching consequences. Organisations should implement countermeasures, in line with their risk exposure, to mitigate an unintentional insider threat.

Intentional or malicious insiders

An intentional insider is an employee who breaches security processes or procedures to purposely cause harm to an organisation.

Intentional, or malicious, insiders may be acting on their own or be recruited by an external party. As insiders they have knowledge of weaknesses within the organisation and how these weaknesses can be exploited.

If acting on their own, an insider may be motivated by ideology, such as being opposed to business decisions, or a feeling that they have been wronged or overlooked within the organisation.

2.2 Know where you might be vulnerable

Bad actors may target public sector agencies and their employees to access sensitive information, or decision-making processes.

These categories are a good way for organisations to assess what resources or information they hold that could be valuable. They can put in place additional security or protective measures. It will also allow organisations to assess where prevention strategies against insider threats might be the most effective.

Information

Identity information is particularly valuable, as it facilitates identity fraud and theft. In some cases it can even lead to witness intimidation, extortion, or can be sold to criminal groups.

The most vulnerable agencies will be those with significant data holdings, particularly those that have access to law enforcement information or large volumes of identity and credit card information. An increasing number of public sector bodies, large and small, collect identity information and could potentially be targeted.

Agencies that have large amounts of data accessable by numerous employees will be most at risk. This may allow malicious insiders to access information while remaining undetected. This is why it is important that security systems are maintained and employees have access only to necessary systems.

Decision-making processes and work areas

Decision making and regulatory processes could be targets for insiders looking to benefit from decisions going their way. This might include decisions around procurement, the awarding of contracts and grants or decisions relating to property and investments. Agencies which process licences or visas can become particular targets. Research from other

jurisdictions has shown the security, construction, gaming and liquor industries present attractive opportunities to fraudsters.

Fraudsters won't limit themselves to one business area. It pays to properly identify, assess and mitigate risks across the entire organisation, and not just the most obvious high risk areas.

Although integrity measures often focus on frontline staff, support officers in administrative and information technology areas may also have access to sensitive information or the ability to conceal improper actions. Where government insiders have carried out malicious acts, we consistently see poor protective security and management processes.

To determine which work areas might face the highest risk, agencies should consider their information, decision-making powers and commodities; vulnerabilities associated with their employees; and work and security practices.

Public bodies must also consider how they share their information and systems. Although a public agency may have identified internal high-risk work areas, they may remain vulnerable where information and systems are shared with other bodies or where functions are outsourced to private providers.

3 Motivations

It is important that employers recognise the triggers for someone carrying out a malicious attack. Sometimes an employee may be struggling financially, or they may have faced a significant life event. But remember, just because one or more of these factors is present it does not always prove malicious intent.

3.1 Financial benefit

Financial benefit is the most common motivation for committing fraud or corruption. A 2016 study conducted by KPMG found that the overriding motivation for corruption was personal financial gain or greed. This may include an employee facing financial difficulty. We often see that gambling or other debts have put pressure on an employee, leading them to become a malicious insider in order to pay off these debts.

The desire for wealth may instead be driven simply by greed. In some instances an employee may want to be perceived as being wealthy and will try to maintain a lifestyle that is beyond their means in order to portray this wealth.

3.2 Workplace discontent

Discontent towards an organisation is a significant motive for the intentional misuse of privilege and access to systems.

In some cases, employees may feel like they have been wronged by an organisation, particularly if they missed out on a promotion, increased remuneration or recognition in their role. Management interventions may further increase an employee's disgruntlement. Some cases of organisational sabotage by insiders have been motivated by revenge following a negative workplace event.

3.3 Remote working

The shift to working from home or flexible working arrangements presents an information security risk, while also creating opportunities for fraud through a lack of oversight. This lack of oversight provides a particularly high risk as employees may accidentally get away with committing fraudulent activity. This may then encourage them to test other methods of taking advantage and lead to more fraudulent activity.

In March 2020 when New Zealand locked down because of the COVID-19 pandemic, many workplaces were forced to rapidly shift to remote working. This left them open to vulnerabilities in new or temporary systems and security controls, especially where they needed to respond quickly to new policies and lockdown measures.

Pressure from financial downturns and job insecurity can also increase fraud risk as employees look to supplement their incomes. Employees facing financial hardship may be more inclined to accept offers from external bad actors, or they might be more motivated to carry out actions they otherwise would not have considered.

Organisations that have now settled into remote working arrangements should carry out pressure testing on new security controls, so that there are effective security measures in place in a future crisis.

Now is the time to pressure test controls, before the next crisis occurs. For more about pressure testing and Managing Fraud During Emergency Relief and Recovery see our website.

3.4 Relationships

Apart from financial benefits, an employee's relationships provide another form of pressure. Family members, friends and members of some communities are drivers for exploitation. Many public servants will feel responsible for maintaining these relationships and the wellbeing of those around them.

Conflicts of interest, not properly managed, can also cause harm to an organisation. Conflicts of interest can arise when private or personal interests run counter to the public interest.

Conflicts are likely to occur through personal, family or community relationships. Under the influence of a corrupt outsider, an employee may unwittingly become a malicious insider. Relationships can also complicate the intention behind a malicious act, with perpetrators becoming unknowing pawns for others whom they may believe are acting innocently.

4 Red Flags

From our case work, the SFO have identified red flags that may indicate that someone is acting maliciously against an organisation. Remember that the presence of any of these common signs doesn't automatically mean you have an insider threat. However, it may pay to speak to someone about it or keep a record of your concerns.

Changes in behaviour/significant life events

- 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 the organisation and its work, or more senior colleagues
- Not wanting to take leave, being nervous about others acting in their position, or 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

5 Responding to insider threats

To adequately detect and deter the risk of an insider it pays to monitor and respond to any suspicious or disruptive behaviours. Regular monitoring can also detect unsuccessful attempts to exceed authorised access.

Sometimes an employee may accidentally breach a security control. If they had previously been seeking to harm an organisation but were unsure how to do so, this breach could encourage them. Ensuring that there are no opportunities for them to act maliciously will help to minimise any ability to sabotage the system.

5.1 Background and pre-employment checks

Comprehensive background checks prior to employment should reveal if previous employers had any concerns.

An organisation should carry out pre-employment checks on everyone, including when employees from within an organisation change roles. This applies particularly to those working in high risk areas such as finance and procurement, and should not be skipped just because of a person's work experience or seniority.

Background checking often relies on the honesty of the employee. It may require them to disclose any potential issues, which they may not always be overly forthcoming about. Checking references thoroughly with previous employers gives you an opportunity to validate any information a potential employee has given you.

For more information on background checking see Public Service Commission – Te Kawa Mataaho - Workforce Assurance Model Standards

5.2 Security controls

The use of technology such as firewalls, access controls and encryption are vital within organisations as they provide a first line of defence against malicious activities.

If security systems and controls are in place, maintain them and keep them up to date. Attempting to predict where an insider might strike is also a valuable way of making sure controls are in place and that they work. This could be done by pressure testing your controls.

Where controls or countermeasures are in place they should be consistently enforced. There should be consequences for employees at all levels where they might have been breached.

Taking a relaxed attitude towards security breaches could provide encouragement to potentially malicious insiders.

Privilege slide refers to someone taking their system privileges with them when they move roles within the organisation. Make sure that access controls are only appropriate for the new role.

Removing privileges as soon as an employee has shifted roles will ensure that access is granted only to the right staff.

5.3 Setting the tone from the top

'Setting the tone from the top' is important for embedding an ethical organisational culture where it is well understood that corrupt or fraudulent behaviours will not be tolerated. The right tone fosters a culture with zero tolerance for all forms of bribery and corruption.

There is a body of evidence showing that ethical culture is a significant determining factor in the amount of misconduct that will take place in a business.

When those in senior positions are seen to uphold the rules, policies and processes of the organisation, those rules are taken seriously by employees. Disregard for these can likewise lead employees to believe that the organisational culture allows such behaviours and that they are likely to get away with them.

Where fraud does occur, evidence suggests that the more senior the employee, the more negative the impact will be on workplace morale. The strength of an ethical culture depends on individuals at each level within the organisation committing to do what is right.

The culture in an organisation plays a role in motivating someone to carry out a malicious act. If decision-makers are transparent in their actions, and show the rationale for their decisions, staff will be less likely to feel resentment.

5.4 Clear avenues for reporting

The *Protected Disclosures (Protection of Whistleblowers) Act 2022* came into force in New Zealand on 1 July 2022 (replacing the *Protected Disclosures Act 2000)*. The Act facilitates the disclosure and investigation of serious wrongdoings in the workplace.

The Act covers a number of integrity issues. It also considers serious wrongdoing to be an act, omission or course of conduct that is unlawful, corrupt or irregular in the use of public

fund or public resources. It seeks to provide protection for those who blow the whistle on malicious insiders.

Reporting by whistleblowers continues to be one of the primary methods of detecting corrupt or malicious conduct by an employee. It is important that staff are able to recognise and feel comfortable reporting suspicious behaviours. Peers, and those working alongside insiders, may be the first to notice any perceived changes in behaviour.

Employers should work to ensure that all employees are aware of the steps they must take if they suspect suspicious behaviour from their colleagues.

COUNTER FRAUD CENTRE

Tauārai Hara Tāware