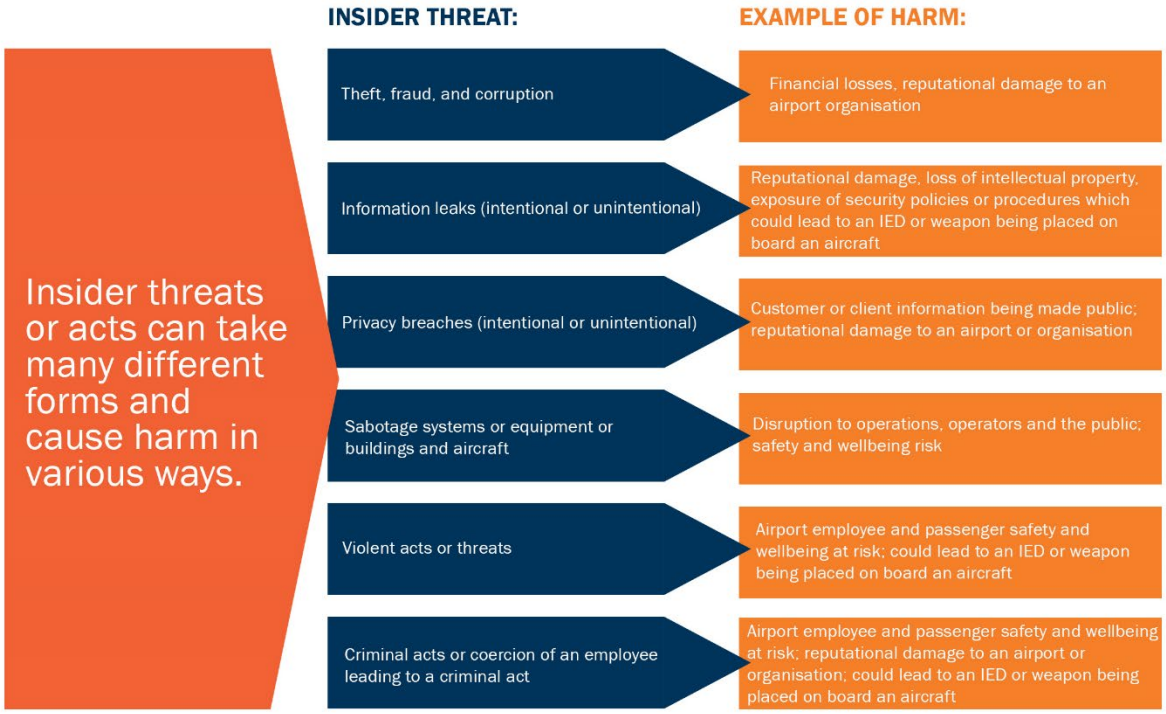
October 2021

In this newsletter

Insider threat

Because we live in a little slice of paradise, we tend to minimise the risk of security threats – and sometimes bad things in general – with 'it won't happen here'. Unfortunately, as we have seen lately, bad things do happen in our country.

Noticing suspicious behaviour in our colleagues, and reporting it, is challenging because we generally think of a stranger when we think of a security threat. But there are plenty of examples around the world – including here in New Zealand – where insiders have taken advantage of their authorised access to an organisation's work location, people, information and systems to do harm.



The intentional insider

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

An intentional insider, who's recruited, is usually responding 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.

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

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

A New Zealand case study

Imitation bomb planted in security area at airport

Just two days after the Christchurch mosque shooting, on 17 March 2019, an imitation bomb was located within the security area at Dunedin Airport. A multi-agency investigation began straight away and identified an Aviation Security Officer employed at the airport was responsible.

The incident caused significant disruption to a large number of passengers and staff when the airport closed. An international flight was forced to return to Australia and several domestic flights were diverted. Defence Force personnel were called to safely destroy the device.

The former employee was found guilty by a jury in November 2020 and was jailed for three years on a charge carrying a maximum penalty of five years.

During the trial, the Crown prosecutor told the jury that on the day in question the former employee undertook a perimeter check as required by his usual duties. During that check he advised his supervisor he wanted to look at an object spotted near a building within the airport perimeter fence. He took a photo of what appeared to be a black bag near the building's entrance. A further inspection treated the bag as 'suspicious'.

Police reviewed access records and CCTV footage. Their investigation revealed the employee had exploited his role to get into restricted areas, including a secure goods room, to get training items that he then used to create the imitation bomb.

The former employee had previously raised concerns over airport security measures and had contacted media about his grievances, as well as circulating petitions about his concerns over security.

The former employee has never acknowledged his actions. The Police, however, believe he was motivated by a desire to increase his income, and that highlighting security concerns would increase his opportunity for increased work hours at the airport.

Watch for signs of anger against your organisation.
Watch for changes in behaviour or performance.
Report concerns or suspicions to your management – they know what to do.

See it. Hear it. Report it.

An international case study

Bomb concealed in a laptop given to a passenger in the sterile area by airport workers

On 2 February 2016 flight DAO159 with 74 passengers onboard took off from Mogadishu in Somalia on a flight to Djibouti. 20 minutes later a bomb disguised in a laptop exploded, killing the person holding it. The professionalism of the crew saved the aircraft. The cabin crew moved all the surviving passengers to the back of the aircraft to make it stable and the flight crew made an emergency landing in Aden.

An investigation revealed the bomb, hidden in a laptop, had been given to a passenger in the sterile area by security staff. An airport worker used their knowledge of the airport to avoid security screening and carried the laptop into the sterile area and handed it to the passenger.

On 30 May 2016, a Somali military court found two men guilty of the plot and to being members of the militant group, al-Shabab. One was a former security official at the airport and the other had financed the attack. They were sentenced to life in prison.

Eight other airport workers, including security screeners, a police officer, a porter and immigration officers were also convicted of helping in the plot.

Don't assume a person in a position of authority won't commit an insider act.
Watch for changes in behaviour and requests for shift changes for no apparent reason.
Report concerns or suspicions to your management – they know what to do.

See it. Hear it. Report it.

The unintentional insider

Unintentional insiders' cause harm accidentally and the most likely cause is poor security behavior or complacency.

An unintentional insider might not know the correct security processes, might ignore security processes (thinking they're 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 unintentional insider acts.

Poor security awareness could mean the unintentional insider:

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

A New Zealand case study

An employee at a New Zealand airport met someone in a bar. The conversation started easily enough but over time the questioning centred on their place of employment. Before they knew it, they had been asked about the number of staff working night shift in the airport, and other aspects of the airport's operation that wouldn't generally be known to those outside the airport environment.

When they realised their mistake, they reported it immediately to their manager and measures were put in place to protect the airport.

We all make mistakes – it's what we do after we've made the mistake that counts!

Don't be the unintentional insider!

Your behaviour contributes to the security of your airport.

'The big six' security measures for large airports

If you work at Auckland, Wellington, Christchurch, Dunedin, Queenstown or Invercargill airports, 'the big six' simple security measures apply to you.

Always wear your airport identity card and make sure it is visible to others.

Check the door closed behind you.

Watch out for tailgaters.

Follow all security policies and procedures.

Know what suspicious behaviour looks like. Question suspicious behaviour.

Report it. It may be part of a bigger picture.

We all contribute - how do your security behaviours stack up?

'The big six' security measures for regional airports

If you work at a smaller regional airport 'the big six' simple security measures for regional airports apply to you.

1

Lock all gates – even if you are there for a short time.

2

Control access to your area.

3

Lock hangars and aircraft (where you can).

4

Follow all security policies and procedures.

5

Know what suspicious behaviour looks like. Question suspicious behaviour.

6

Report it.
It may be part of a bigger picture.

We all contribute - how do your security behaviours stack up?

Protecting yourself and others from an insider threat

Recognise the four most common beliefs preventing you identifying an insider threat –

- there's **no real danger** from insider threat and the harm it can cause
- **'none of my colleagues are capable of committing insider acts'**
- it's **against Kiwi culture to dob in a colleague** we suspect of committing insider acts
- day-to-day job pressures make people **too busy** to follow proper security procedures and behaviours.

These beliefs aren't always easy to change, but to keep ourselves, our colleagues and our passengers safe, we need to recognise threats have changed and we need to change with them.

We all contribute to airport security!

To read previous security culture newsletters, visit our security culture webpage.