

What are the threats to my business?

Kia rite, kia ū, kia matāra

A threat is any source of potential harm or disruption that is a risk to your business. Threats can come from a range of sources, including:

- state-sponsored actors who undertake political and economic espionage in Aotearoa New Zealand
- criminal groups who may seek to control access to your systems so they can extort you for money, in exchange for returning control
- other cybercrime actors looking to scam individuals through fraudulent online activity.

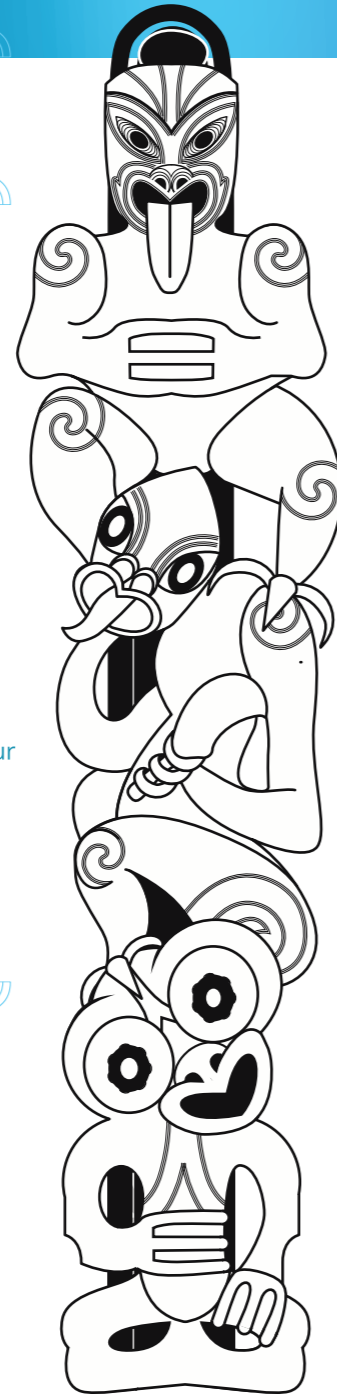
In 2024, the average cost per incident reported to the NCSC was \$25,500

Losing money to cyber attacks and scams has an impact on your business. You could miss out on the chance to invest that money into growing your business for future generations.

In serious cases, cybercrime actors could take control of key assets owned by Iwi Māori which would undermine the ability for Māori to protect and govern them.

Threat actors may use your people, information, or assets to commit cybercrime, or conduct foreign interference and espionage which could:

- prevent you from operating your business
- lead to misuse or mishandling of information (either deliberately or accidentally)
- erode the trust and confidence your community and your customers have in you
- harm your people or lead to a loss of information or assets.



What do I need to protect?

Tiaki tāngata Protecting people

Protect your people from threats that may harm them or your business

Your tāngata may include:

- Employees
- Contractors
- Suppliers
- Volunteers
- Other building tenants

To protect your people you should:

- **Make background checks part of your recruitment process** so that you can feel confident they are someone you can trust
- **Build a security culture** in the workplace where security incidents can be openly talked about and learned from
- When an employee leaves your business, **remove their access** to your sites and systems

Tiaki taonga Protecting assets

Keep taonga safe and secure for future generations and for future prosperity

Your taonga may include:

- Products
- Property
- Buildings
- Vehicles
- Workplaces
- Home office

To protect your assets you should:

- **Identify your assets** and where they are located (your most valuable assets are the things that you could not do business without)
- **Secure your assets** with physical barriers and make sure you can see who is accessing them (even when you're not around)
- **Control access to your assets** using control and monitoring systems to ensure access is only available to people who need it

Tiaki mātauranga Protecting information

Store, protect, and process your information responsibly

Your mātauranga may include:

- Customer records
- Personal information
- Banking credentials
- ICT systems

To protect your information you should:

- **Keep your software up to date** to ensure your environment stays secure
- **Enable multi-factor authentication** on sensitive accounts to protect your business information from unauthorised access
- **Backup your data** to ensure you can get it back quickly and easily if it is lost or stolen

What should I consider?

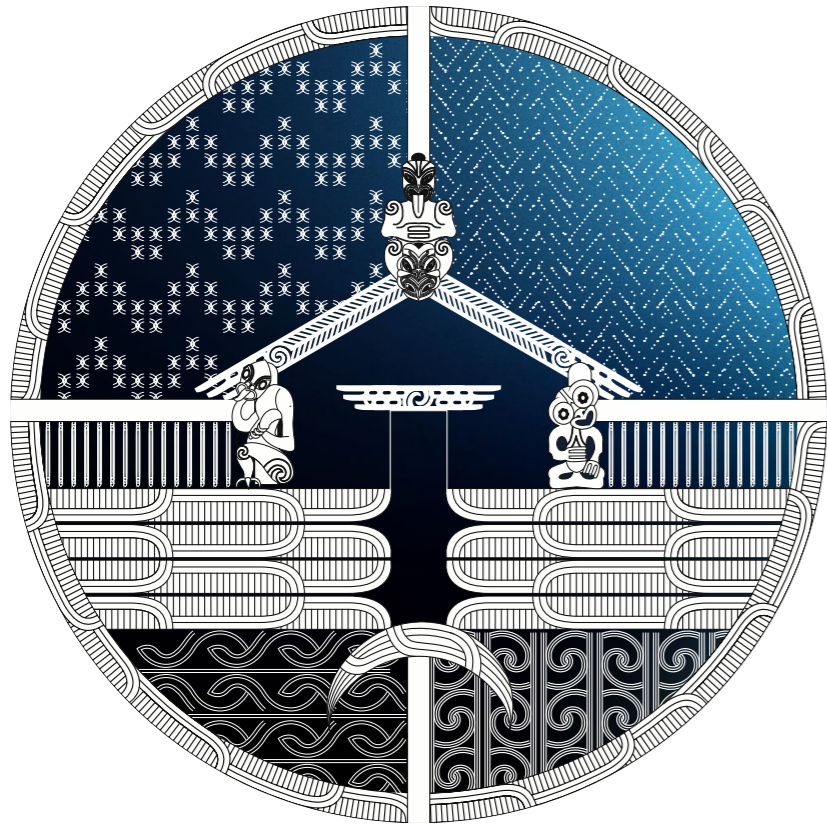
- Are pre-employment background checks part of your recruitment process?
- What level of pre-employment checks do you do on contractors and service providers?
- Does your business have a formal document outlining the security culture? Does it include security responsibilities for employees?
- What security training and support do employees get?
- What are the key security messages for employees and how are they communicated?
- Are contractors and suppliers aware of what their security responsibilities are in the workplace?
- Do you conduct security surveys?

- Do you have a record of your most valuable assets and where they are?
- Do you know who has access to your workplace and how often they access it?
- Who controls who has access to your workplace and assets? Are these access points monitored and protected?
- How does access control differ for different people, e.g. visitors, employees, delivery persons?
- How do you know your assets are properly protected?
- Are any of your contractors or suppliers responsible for your most valuable assets?

- What data does your business store that needs to be protected?
- Who may want access to the systems and data your business has?
- What software and systems does your business use that could be vulnerable? How can you secure these?
- Who in your business needs access to specific systems and data to do their job?
- Are you providing the security tools your employees need to operate securely, e.g. multi-factor authentication, password management?
- Do you have an incident response plan ready if something happens?

What is protective security?

In an increasingly complex world, keeping ourselves and each other safe is more important than ever.



Protective security is like the pā that keeps a hapū safe.

At the heart of the pā stands the whareniui where tāngata, mātauranga, and taonga are held – people, information, and assets. There are many layers of the pā that protect the whareniui – palisades and trenches, as well as tikanga and kawa.

Protecting tāngata, mātauranga, and taonga from harm helps businesses carry out their mahi.

Just like the pā that protects the whareniui, your business should be strong, well-maintained, and able to resist attack.

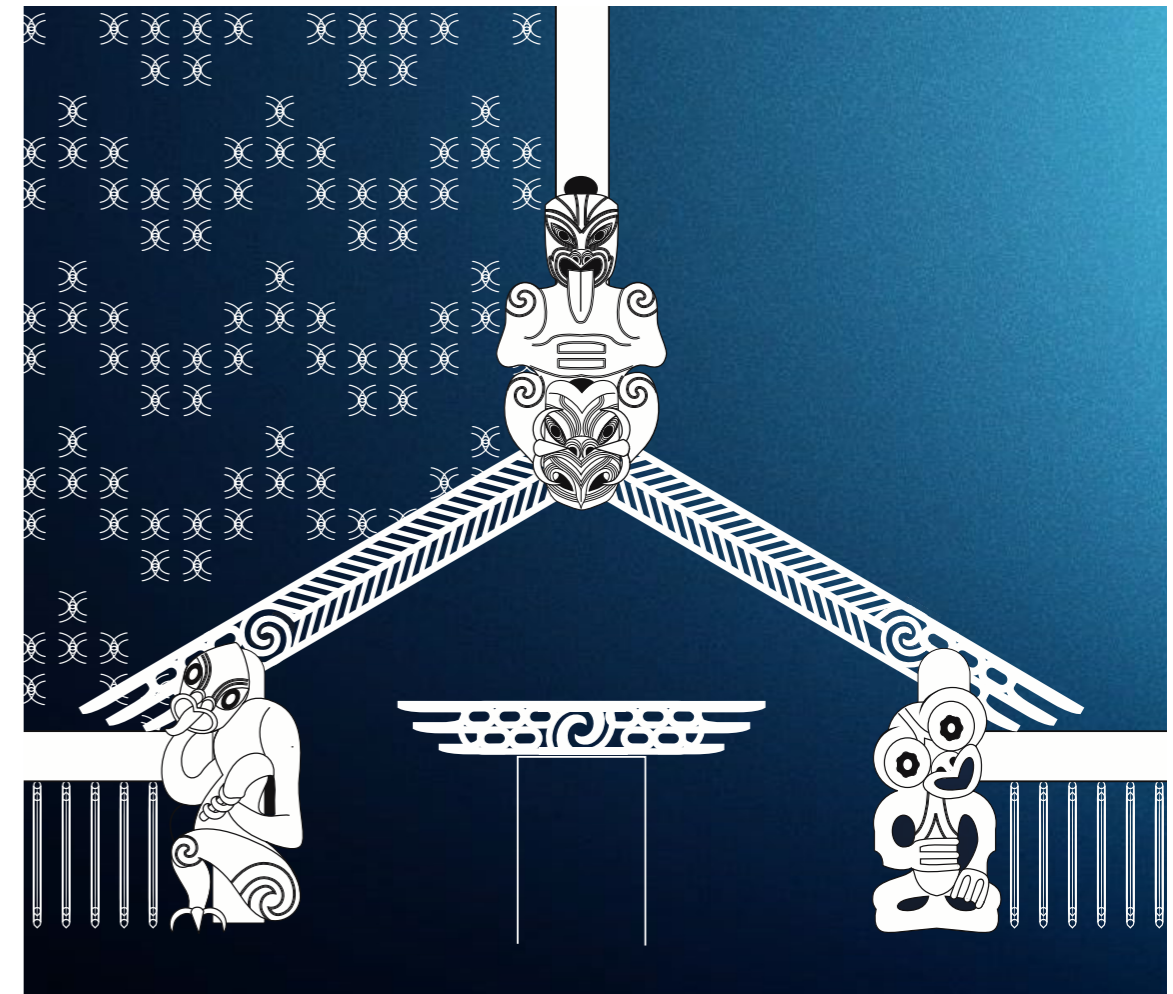


Learn more about protective security

protectivesecurity.govt.nz/tiaki

Tiaki Pakihi Māori

Protective security for Māori business and entities



PSR | Protective Security Requirements

National Cyber Security Centre