Te Tira Tiaki
Government Communications
Security Bureau

Te Pā Whakamarumaru
New Zealand Security
Intelligence Service

SECURE INNOVATION

SECURITY ADVICE FOR EMERGING TECHNOLOGY COMPANIES

National Cyber
Security Centre

PSR
Protective Security
Requirements

FOREWORD

New Zealand is a country of innovators.

Our technology sector has grown to become our third largest exporter, contributing $23 billion to our gross domestic product in 2023. We have built a reputation for our openness, our ingenuity, and our willingness to collaborate.

Success can come with risks, and it is important that we recognise the threat of economic espionage. We are no longer operating in a benign environment. Your innovative breakthroughs can make you a target. A range of state and criminal actors are likely seeking to gain commercial, technological, or military advantage off the back of your hard work.

Our security intelligence agencies and their partners across the Five-Eyes are being more open about the nature of the threat. Now it is up to the technology sector to also help to manage the risk, build resilience and adopt more of a security mindset.

Security need not inhibit innovation – rather it can foster and protect it. If you are operating in a secure way, you may be more attractive to investors, leading to greater potential for growth.

This guide outlines straightforward advice to help you embed strong security practices and ensure you collaborate with other organisations here and around the world securely. I encourage any technology company in New Zealand – large or small – to consider this advice and make it part of how you do business.

Hon Judith Collins KC

Minister Responsible for the GCSB
Minister Responsible for the NZSIS
Minister of Science, Innovation and Technology
Attorney-General
Minister of Defence
Minister for Space
Minister for Digitising Government

CONTENTS

SECURITY FROM THE START

This guidance is intended for founders and leaders of startups in the emerging technology sector.

Good security practices can protect your competitive advantage and make your research, intellectual property, or company more attractive to investors and customers. This guide outlines cost-effective measures you can take now to protect your ideas, reputation, and future success.

This advice for emerging technology companies in Aotearoa New Zealand has been published at the same time as similar guidance from security intelligence agencies in Australia, Canada, the United Kingdom and the United States. It is part of a joint effort to help protect our technology sectors from a range of current and emerging threats, particularly those from state actors.

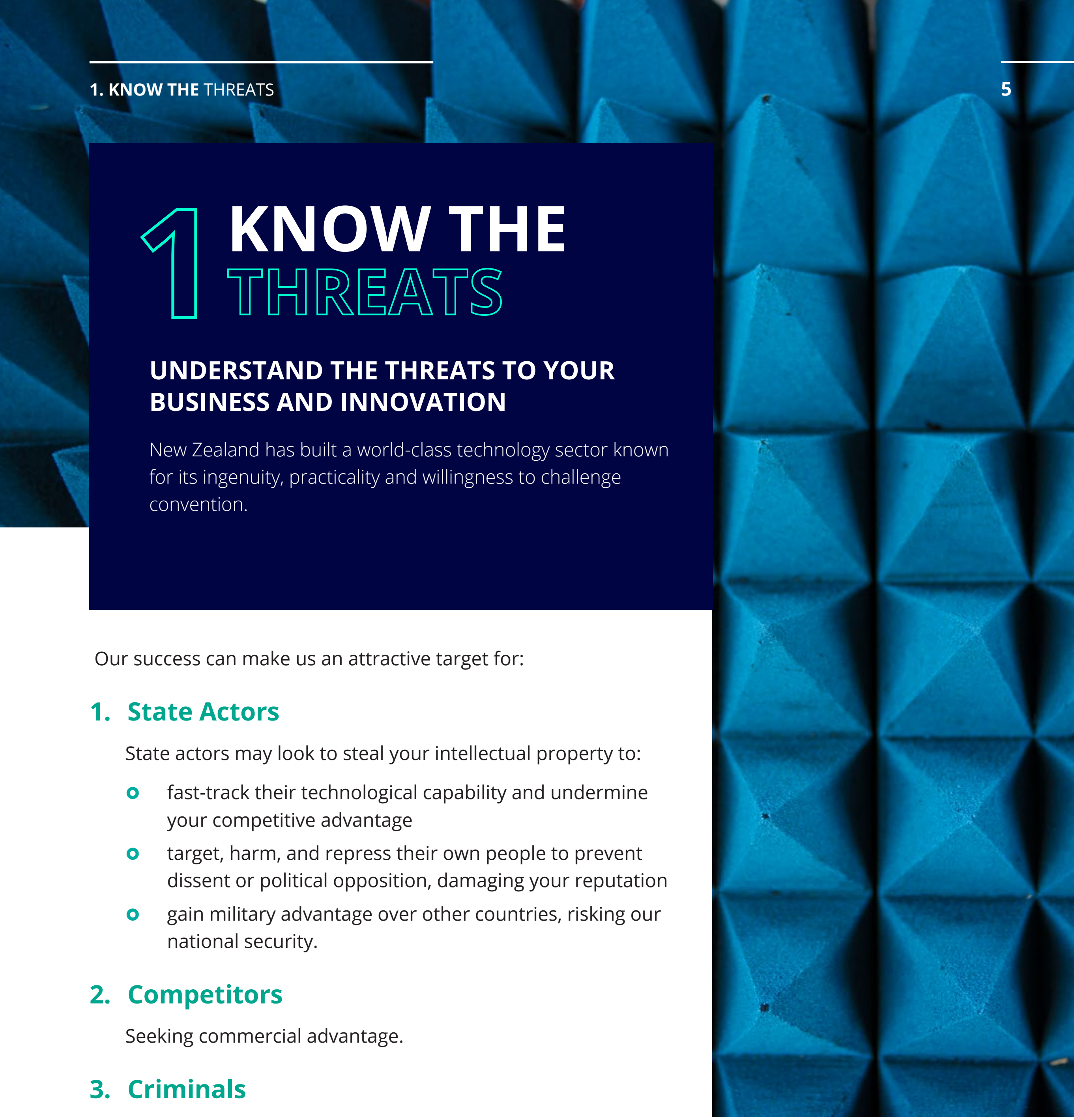
Laying strong foundations now will help your security to be more effective and less costly as your business grows in the future. Following the five secure innovation principles set out in this guide is a great first step for any innovator looking to protect their hard work from those who wish to steal it.

Secure innovation principles

1. **Know the threats** – understand the potential vulnerabilities that might put your product or innovation at risk.
2. **Secure your business environment** – manage the security risks your business faces.
3. **Secure your products** – ensure the products and services you are developing are secure and that you are actively protecting and managing your intellectual property and expertise.
4. **Secure your partnerships** – operating securely means managing the risks that come with partnerships with investors, suppliers and collaborators.
5. **Secure your growth** – account for additional security risks as your company grows.

This guide provides a framework for considering security risks and includes links to information to help you apply these principles.

Taking the right steps now will help you to embed good security practices from an early stage, making your business more robust and resilient.



1 KNOW THE THREATS

UNDERSTAND THE THREATS TO YOUR BUSINESS AND INNOVATION

New Zealand has built a world-class technology sector known for its ingenuity, practicality and willingness to challenge convention.

Our success can make us an attractive target for:

1. State Actors

State actors may look to steal your intellectual property to:

- fast-track their technological capability and undermine your competitive advantage
- target, harm, and repress their own people to prevent dissent or political opposition, damaging your reputation
- gain military advantage over other countries, risking our national security.

2. Competitors

Seeking commercial advantage.

3. Criminals

Looking to profit from companies with weak security practices to steal data relating to your assets, customers and people.

KNOW YOUR POTENTIAL VULNERABILITIES

There are a number of methods malicious actors may use against you.

- **Insider access** – Your people are your greatest asset, but in some cases, they can pose a risk of insider threat.
- **Cyber access** – Insecure IT can provide an easy way for your business to be exploited.
- **Physical access** – Tangible or digital assets could be stolen directly from your place of work.
- **International travel** – State actors can operate more easily overseas than in New Zealand.
- **Investment** – Investment can be used to gain access to, and influence over, your company.
- **Overseas jurisdictions** – International expansion exposes you to security risks from local laws and foreign business practices.
- **Supply chain** – Vulnerable or malicious suppliers could compromise your business.

Take the time to understand and think through how different threats can impact your business.

No organisation can eliminate all threats they face, but it is possible to manage the risks.

Your security measures should consider ways to protect your people, information, and assets.

Learn more about the threat environment and how it may affect you:

- New Zealand's Security Threat Environment – NZSIS's independent assessment of the threats we face from foreign interference, espionage, insider threat, violent extremism and terrorism. – *New Zealand Security Intelligence Service*
- Cyber threat report – actionable insights into New Zealand's cyber threat environment, including mitigations to recurring tactics used by malicious actors – *National Cyber Security Centre*

2 SECURE YOUR ENVIRONMENT

PROTECTIVE SECURITY REQUIRES MANAGEMENT OF YOUR SECURITY RISKS

Protective security is a series of risk management measures designed to help organisations and communities protect their people, information and assets. Effective security enables organisations to work together securely in an environment of trust and confidence.

When managing your security risks, consider:

2.1 **Ownership** – Who will lead and be accountable for your security?

2.2 **Identification** – Which assets are most critical to your success?

2.3 **Assessment** – What's your level of security risk?

2.4 **Mitigation** – How can you lower your risk level?

2.5 **Foundations** – How can you make security part of your business?

2.1 OWNERSHIP LEAD BY EXAMPLE

→ Identify a security lead at the leadership, Board, or senior level where possible

→ Start talking about security from the start so it is normalised as part of your business

Identify someone who is responsible for security to ensure that it becomes factored into your business decisions.

The startup phase is the perfect time to set the tone for your security culture, although it is never too late. Open and ongoing conversations about how to protect your most important information and assets are vital for fostering a positive culture in which your people feel comfortable to report incidents and learn from them. These discussions will foster a shared understanding about what most needs protecting and your levels of tolerance to risk.

Governance is a set of activities that enables your organisation to make sound security decisions.

Security governance activities may include:

- defining the principles of a security programme
- providing a holistic view of risk
- actively monitoring performance.

Your governance function sits with your board or senior leadership who can ensure the right investment is made, at the right time and in the right place.

2.2 IDENTIFICATION KNOW WHAT NEEDS PROTECTING

→ Identify your most valuable assets that are critical to your existence and future success

Identifying the assets which are critical to your success should be the starting point in your security planning.

Your innovation or intellectual property will likely go straight to the top of your list – but also consider what led to your breakthrough.

The information and assets you consider critical may be wider ranging than you think. They may include tangible assets such as your buildings, equipment, and key people, or intangible assets such as ideas, software, brands, expertise, relationships, or know-how.

2.3 ASSESSMENT

ASSESS SECURITY RISKS ALONGSIDE OTHER RISK TO YOUR BUSINESS

→ Understand the potential threats to your critical assets

A good assessment of the threats you face and sound management of your risks will make you more attractive to potential customers and investors.

Consider these security risk scenarios:

○ Theft or unauthorised access to your information or assets at your premises, by an employee, visitor, or external party

○ Theft or unauthorised access to your information or assets during travel

○ Theft or unauthorised access to your information or assets from a remote location

○ Intellectual property loss from partnerships.

01

Case study

A New Zealand technology business was engaging with a potential new customer. In the course of this engagement, the New Zealand business carried out basic due diligence, which revealed the customer had not disclosed links to a foreign state. Based on this, the business decided to not take the relationship any further. These actions prevented a probable attempt by a state actor to obtain access to the business's technology. Good security practice avoided credible risks to the company's reputation and competitive advantage.

2.4 MITIGATION LOWER YOUR LEVELS OF RISK

→ Put in place mitigations to reduce your risks to acceptable levels

→ Establish a process to review risks regularly

Completing a risk assessment will help you identify vulnerabilities and the potential impact of exploitation.

We also recommend:

- establishing a security strategy for your business based on an understanding of your key assets, the risks they face, and the risks you are willing to tolerate
- regularly reviewing security policies and procedures so that they evolve with your exposure to new threats
- establishing responsibilities for security with any new employees, contractors, or suppliers.

Further information

Learn more about securing your environment:

+ Security governance advice – eight governance requirements to ensure effective oversight and management of all areas of security – *Protective Security Requirements*
+ Charting your course: cyber security governance – six steps to improving your governance and becoming more cyber resilient – *National Cyber Security Centre*

2.5 FOUNDATIONS MAKE SECURITY PART OF YOUR BUSINESS

Part of securing your environment is making security part of your business. Consider how you will protect your people, information, and assets at the same time.

BUILD SECURITY AROUND YOUR MOST CRITICAL ASSETS

Place barriers (physical or virtual) around each asset you have identified as needing protection.

Restrict access to people who need it and are trusted to use it securely, by using things like swipe card access or restricting permissions.

Detect unauthorised activity around your assets to help avoid security incidents.

Take regular backups of critical data and keep them physically and logically separate from your main system. This will allow you to continue to work following the impact of any physical damage, theft, or ransomware attack.

BUILD IN BASIC IT SECURITY WHEN SETTING UP YOUR SYSTEMS

Insecure IT can provide an easy way for your business to be exploited. Follow these steps to reduce the likelihood and impact of your systems being breached.

Switch on your firewalls and antivirus

Most popular operating systems now include a firewall, so it may simply be a case of switching this on. Similarly, antivirus software is often included free, and should be used on all devices.

Use passwords to protect devices and accoUnts

Use password protection or other methods to 'lock' your devices (such as a fingerprint, PIN, screen-pattern, or face recognition). If your devices come with default passwords, change these before they are distributed to staff.

- Use multi-factor authentication (MFA) – for ‘important’ accounts (e.g. email or banking). This uses two methods to ‘prove’ your identity, usually a password and something else such as a code sent to your phone.
- Avoid using predictable passwords (such as dates or names) or common passwords that can be guessed easily.

Keep devices and software up to date

Make sure all IT equipment software and firmware is kept up to date. These updates will not only add new features, but they will also patch any security holes that have been discovered.

Wherever there is an option to do so, set systems to automatically update. Once a product reaches the end of its supported life and these updates are no longer available, consider replacing with a more recent device.

Think about how you connect to the internet

Consider the risks of connecting devices to unknown public Wi-Fi hotspots. Doing so could allow the provider (who may not be who you think it is) to see what you're doing and to access your private login details. Instead, use your mobile network which will have built-in security, preferably in conjunction with a virtual private network (VPN).

- If you need to routinely access the internet over untrusted infrastructure, you should consider using a VPN. Take care to understand what you are paying for and how your connection to the internet is made.
- If you are using an internet connection provided as part of shared office space, consider how confident you are in both the provider and any other parties sharing the connection.

Enable tools to track, lock, or wipe lost or stolen mobile devices

You or your employees are more likely to lose devices such as tablets or phones, or have them stolen, when away from the office or home. Fortunately, most devices include free web-based tools you can use these tools to:

- track the location of a device
- remotely lock access to a device (to prevent anyone else using it)
- remotely erase the data stored on a device
- retrieve a backup of data stored on a device.

Learn more about basic IT security:

+ Business online security assessment tool develop a customised action plan to become more secure online – *Own Your Online*
+ Cyber Security Framework ways to think about, talk about, and organise cyber security efforts – *National Cyber Security Centre*
+ Applying business impact levels – Design and implement security measures that are in line with your risks – *Protective Security Requirements*

Further information

3 SECURE YOUR PRODUCTS

BUILD SECURITY INTO YOUR PRODUCTS FROM THE BEGINNING

Ensure the information and assets you have and are developing are secure.

It is recommended technology start-ups use Secure by Design and Secure by Default principles in the design phase. This helps you make sure security problems are addressed at their root cause. These principles are designed to help you remove security vulnerabilities that can limit your success.

Secure by Design

Security is integrated from the start of the development process to minimise vulnerabilities.

Secure by Default

Out of the box security configuration where no additional action is required to ensure security.

Protect your intellectual property

Intellectual asset and intellectual property management strategies are essential for any business and should be integrated with your business plan. Understanding the assets you have and what you want to do with them will help determine the actions required. You need to understand:

1. What you need to protect
2. How you need to protect it
3. The laws of the countries in which you plan to operate
4. How you are going to manage your intellectual property.

3.1 MANAGE YOUR SUPPLY CHAIN

→ Protecting your information in a digitally connected world demands an understanding of third-party vendor supplier security.

Think about:

- Who is in your supply chain – do you trust the hardware, software, services, or materials you receive?

Choose secure and verifiable technologies

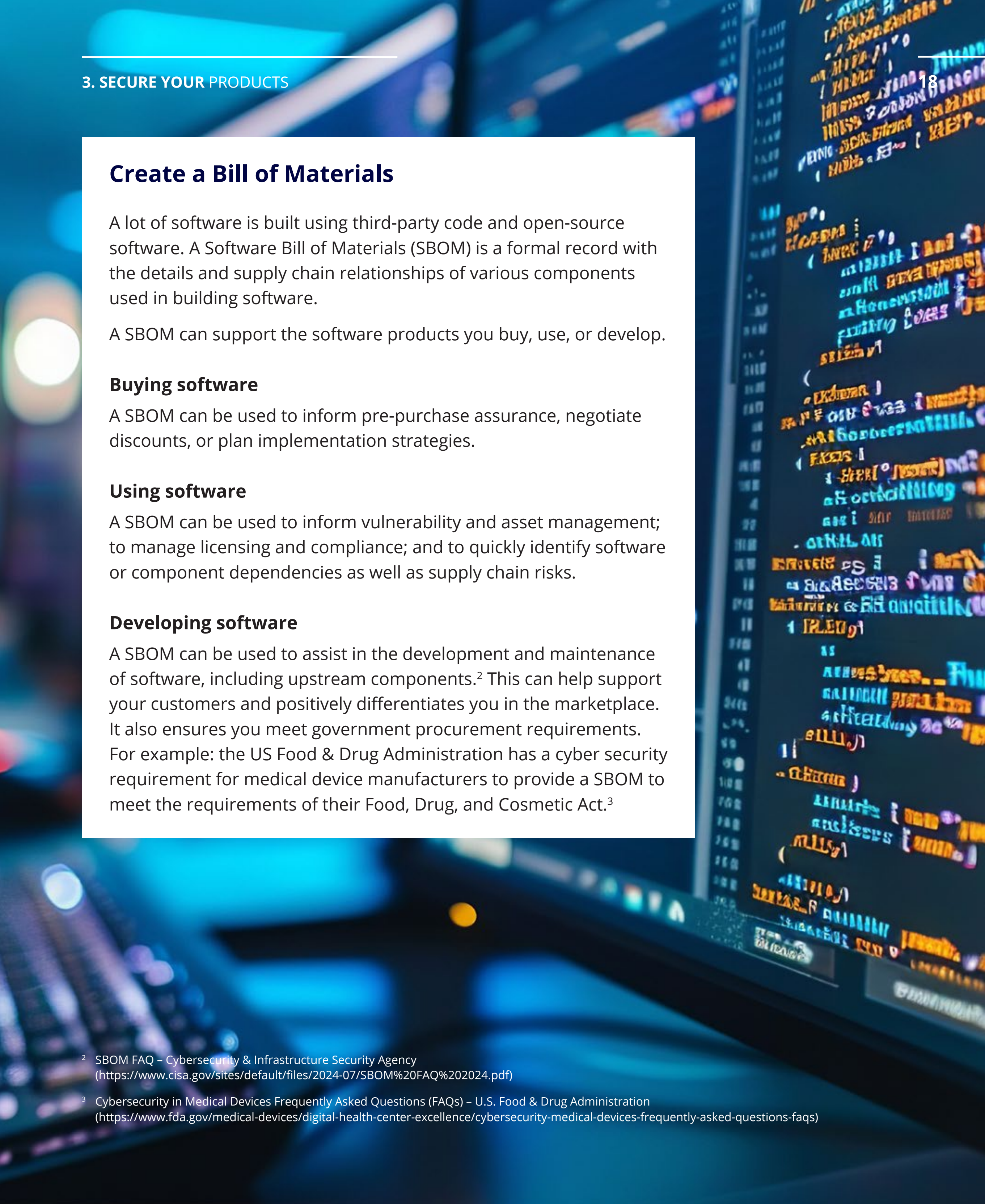
When you need to buy a digital product or service, consider whether the product or service is secure now and will continue to be secure throughout its useful life. Proactive integration of security into your procurement process can significantly mitigate risk and reduce cost.[1]

Further information

Learn more about securing your products:

+ Intellectual property protection for NZ businesses – learn how to protect the value of your product or service and brand with intellectual property rights – *New Zealand Trade and Enterprise.*
+ Cyber Security Investment – provides a structured approach to investing in your cyber security and shows how to manage a delivery programme that is aligned to your strategic and financial governance – *National Cyber Security Centre*
+ Principles for security-by-design and -default – a cyber security roadmap for manufacturers of technology – *National Cyber Security Centre*
+ Secure-by-Design: Choosing secure and verifiable technologies (joint guidance) – helping procurement organisations make informed, risk-based decisions – *National Cyber Security Centre*
+ Supply chain cyber security – outlines three key phases to build capability and manage risk – *National Cyber Security Centre*

[1] Joint Guidance: Choosing Secure and Verifiable Technologies – *National Cyber Security Centre* (https://www.ncsc.govt.nz/news/choosing-secure-and-verifiable-technologies)



Create a Bill of Materials

A lot of software is built using third-party code and open-source software. A Software Bill of Materials (SBOM) is a formal record with the details and supply chain relationships of various components used in building software.

A SBOM can support the software products you buy, use, or develop.

Buying software

A SBOM can be used to inform pre-purchase assurance, negotiate discounts, or plan implementation strategies.

Using software

A SBOM can be used to inform vulnerability and asset management; to manage licensing and compliance; and to quickly identify software or component dependencies as well as supply chain risks.

Developing software

A SBOM can be used to assist in the development and maintenance of software, including upstream components.[2] This can help support your customers and positively differentiates you in the marketplace. It also ensures you meet government procurement requirements. For example: the US Food & Drug Administration has a cyber security requirement for medical device manufacturers to provide a SBOM to meet the requirements of their Food, Drug, and Cosmetic Act.[3]

[2] SBOM FAQ – Cybersecurity & Infrastructure Security Agency (https://www.cisa.gov/sites/default/files/2024-07/SBOM%20FAQ%202024.pdf)

[3] Cybersecurity in Medical Devices Frequently Asked Questions (FAQs) – U.S. Food & Drug Administration (https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity-medical-devices-frequently-asked-questions-faqs)

4 SECURE YOUR PARTNERSHIPS

MANAGE THE RISKS THAT COME WITH COLLABORATION

- → Balance opportunity with risk when collaborating with new partners such as investors or suppliers.
- → Consider security as part of your investment strategy.

New Zealand has an open economy, and building partnerships and opportunities for collaboration is a big part of how we do business.

As New Zealand's security environment continues to evolve, it is important for you and your business, no matter the size, to understand the risks to your business operations including when building international partnerships.

Partnerships increase the number of external routes into your organisation, and to any information or assets you may share. To help you grow safely, you should manage the additional risks that collaboration brings.

Think about:

1 Why you are collaborating

Define your purpose and consider outcomes, benefits, and red lines.

2 Who you are working with

Conduct due diligence assessments on potential investors, suppliers, and collaborators to understand their background and motivations.

3 What you are sharing

Be strategic about what and when you share with partners. Set up your systems so sensitive data is not accessible to your wider organisation or external parties.

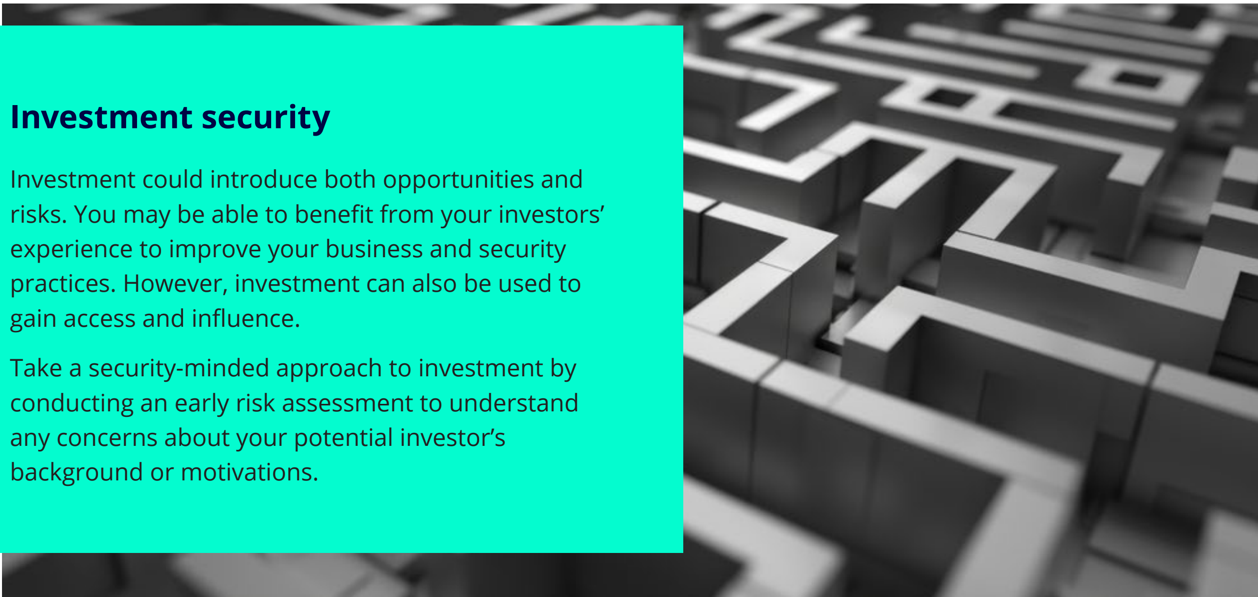
Consider how you will get your information back at the end of a collaboration

4 How you are protecting your innovation

Include protections for your assets and data within contracts.

Consider using non-disclosure agreements to restrict the use of your ideas and information to a specific permitted purpose

It is also worth considering that your early choice of partners – whether they be investors, customers, or suppliers – may have an impact upon who is willing to do business with you later.



Investment security

Investment could introduce both opportunities and risks. You may be able to benefit from your investors' experience to improve your business and security practices. However, investment can also be used to gain access and influence.

Take a security-minded approach to investment by conducting an early risk assessment to understand any concerns about your potential investor's background or motivations.

02

Case study

A New Zealander was recruited by an overseas university where they worked on projects which advanced a foreign state's military capability. Later, they were linked to an agreement to host a talent recruitment station in New Zealand, intended to benefit the same foreign state. While international partnerships are often positive, in this case a foreign state had the opportunity to exploit legitimate arrangements to covertly obtain technology, intellectual property or expertise for a state's military or strategic benefit.

Overseas investment regime

New Zealand's Overseas Investment Act requires a review of investments in strategically important businesses that may pose a national security risk.

Businesses involved in producing sensitive technologies that have military or dual-use applications require new, and in some cases repeat, overseas investors to undergo mandatory national security screening. Businesses that develop, produce or maintain access to significant amounts of sensitive information may also be subject to screening.

Both the New Zealand Security Intelligence Service and Government Communications Security Bureau support the Overseas Investment Office to provide advice on such transactions to ensure our national security is not compromised.

Further information

Learn more about securing your partnerships:

- Due Diligence Assessments for foreign interference and espionage threats helps organisations identify and mitigate the risks when working with others – *Protective Security Requirements*
- Overseas investment Guidance – rules for investing in New Zealand, for both buyers and sellers – *Toitū Te Whenua Land Information New Zealand*
- Using reciprocal confidentiality agreements how to use a signed agreement to prevent sensitive information from being disclosed or misused – *New Zealand Trade and Enterprise*
- Managing Inwards Visits – helping New Zealand organisations assess possible security risks around visiting delegations from overseas – *Protective Security Requirements*
- Guidance for High-Profile Individuals – outlines cyber security measures for high-profile people – *National Cyber Security Centre.*

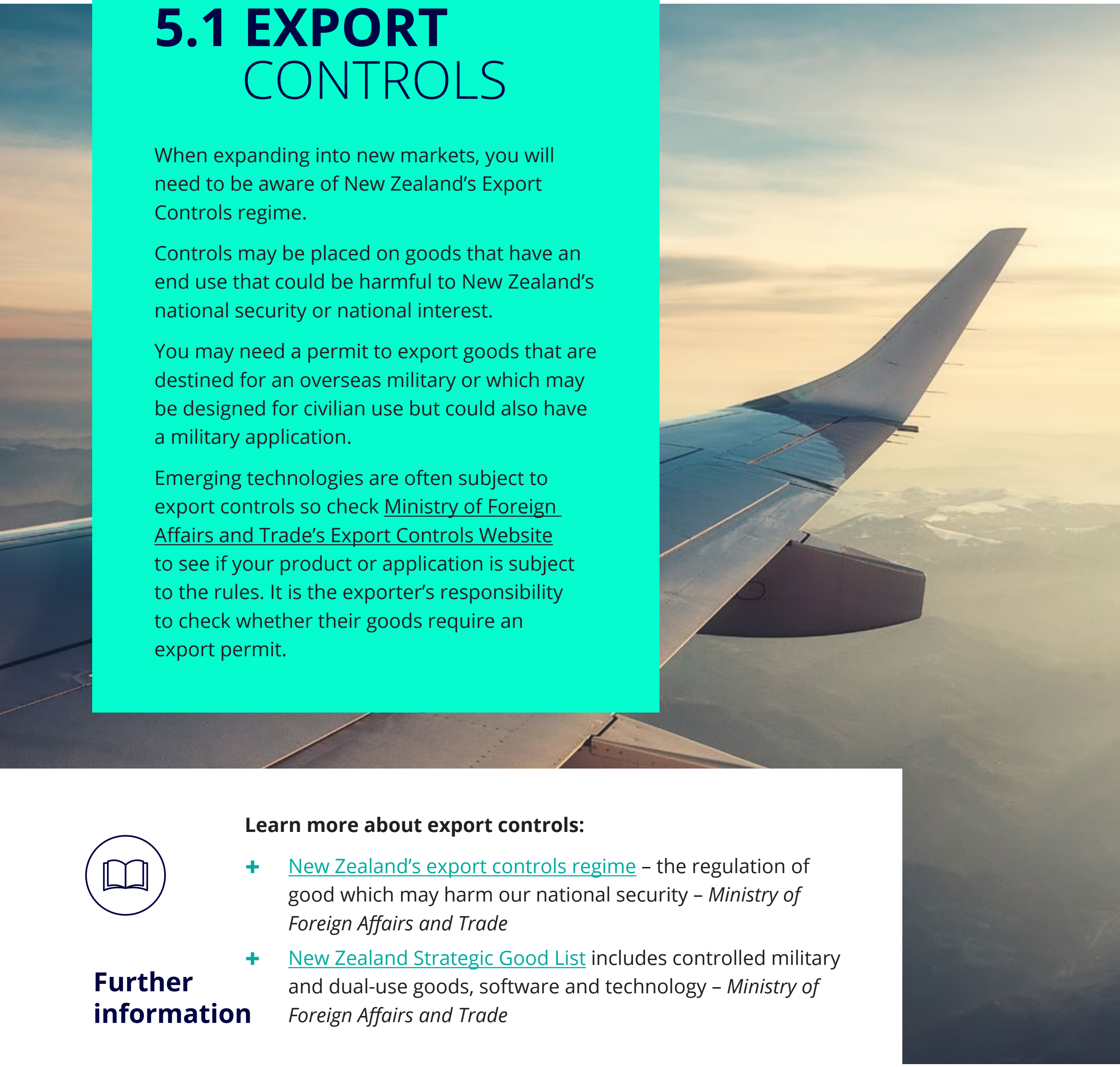
5 SECURE YOUR GROWTH

EXPAND SAFELY INTO NEW MARKETS

- Comply with export controls
- Understand how local laws could increase the risk to your business
- Implement security procedures for your international travel
- Develop and maintain a positive security culture as you grow your team

As your company evolves, so too should your security measures. The risks you face may change as you enter new markets, seek more investment, employ more staff and move into bigger premises.

You should regularly review your security measures to understand whether you need to take additional precautions.



5.1 EXPORT CONTROLS

When expanding into new markets, you will need to be aware of New Zealand's Export Controls regime.

Controls may be placed on goods that have an end use that could be harmful to New Zealand's national security or national interest.

You may need a permit to export goods that are destined for an overseas military or which may be designed for civilian use but could also have a military application.

Emerging technologies are often subject to export controls so check Ministry of Foreign Affairs and Trade's Export Controls Website to see if your product or application is subject to the rules. It is the exporter's responsibility to check whether their goods require an export permit.

Further information

Learn more about export controls:

+ New Zealand's export controls regime – the regulation of good which may harm our national security – *Ministry of Foreign Affairs and Trade*
+ New Zealand Strategic Good List includes controlled military and dual-use goods, software and technology – *Ministry of Foreign Affairs and Trade*

5.2 LOCAL LAWS

It is important to understand the local laws in the countries where you plan to operate.

Different countries have different export control laws, as well as laws regarding the handling and storage of intellectual property. National security laws in foreign countries can allow that country's government to access data or information stored in, or transmitted via, that country.

Understanding local laws will ensure that you are legally compliant, and that you understand the additional security risks involved in expansion into new markets.

Further information

Learn more about lawful access:

+ Lawful access to official data offshore – high-level information about how data can be accessed lawfully in jurisdictions outside of New Zealand – *National Cyber Security Centre*.

Foreign national security laws

New Zealanders should be aware that the People's Republic of China (PRC) has strict laws in relation to national security which may be interpreted broadly. Key concepts like 'state security', 'national interest', and 'state secrets' have wide-ranging definitions in Chinese law. The PRC can compel companies and citizens to cooperate with national security directives. New Zealand businesses operating in China are subject to these same laws and would be required to cooperate if authorities requested access to information, data and systems.

THINK ABOUT WHAT TO SHARE, TRADE, AND PROTECT

5.3 SAFE TRAVEL

As you grow, you may need to travel internationally. Consider whether planned travel is likely to introduce additional risks and take appropriate steps to mitigate them.

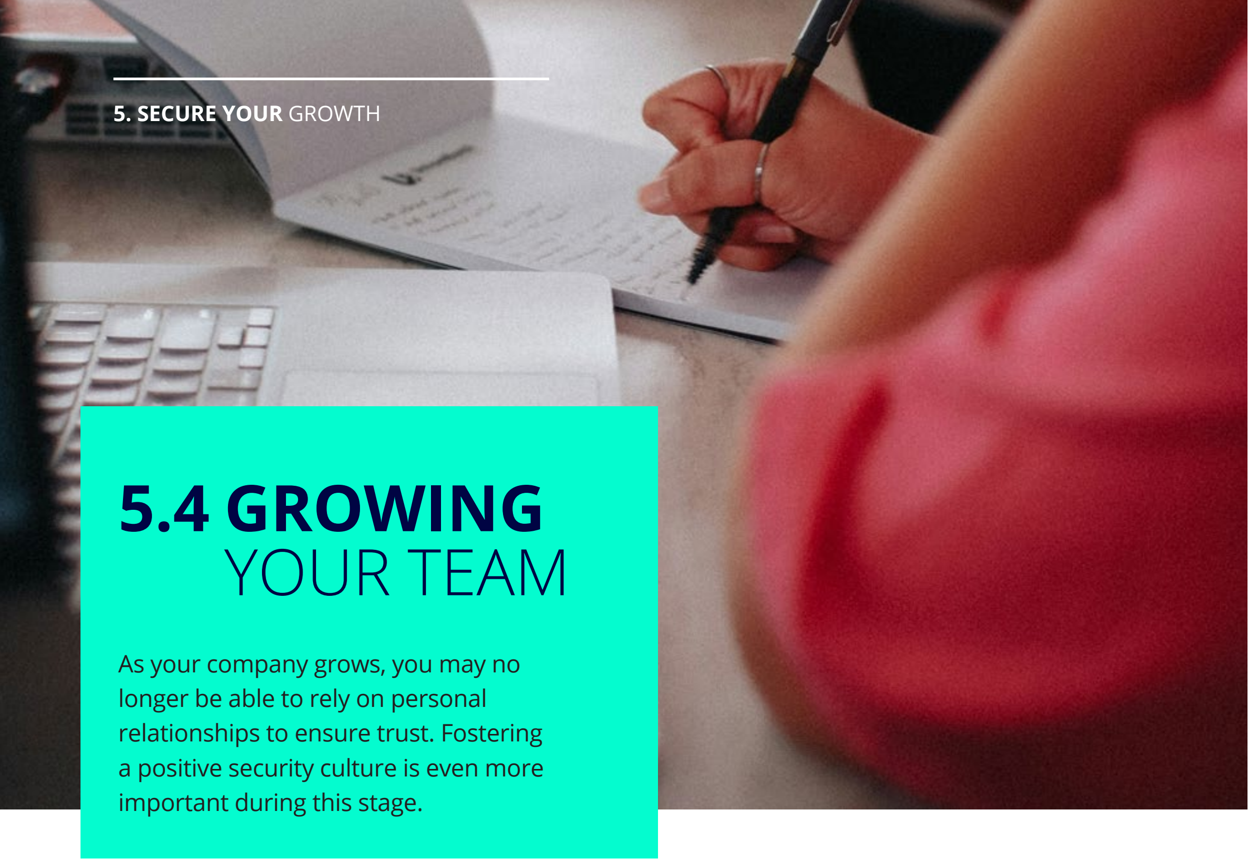
Think about:

- why you might be targeted
- how you might be targeted
- how you can minimise the risk.

Further information

Learn more about travelling safely:

- Security advice for New Zealand Government officials travelling overseas on business – *Protective Security Requirements*
- Official advice for New Zealanders living and travelling overseas – *Safetravel.govt.nz*



5.4 GROWING YOUR TEAM

As your company grows, you may no longer be able to rely on personal relationships to ensure trust. Fostering a positive security culture is even more important during this stage.

Consistency and communication are vital in creating an environment where people feel empowered to speak openly. This means making it easy and routine to report any concerns, handling those concerns sensitively and without blame, and keeping those involved informed of both the progress and benefits of any resulting actions to reinforce confidence in reporting.

Providing ongoing security training, including at the point of induction, for your team will also help maintain your security culture. Effective education and training will help individuals to understand what policies, standards, and procedures are in place to maintain security.

A role-based security risk assessment will help you keep your security measures proportionate and effective. You should have already assessed the risks to your business based on the likelihood and consequence of any threat to your information and assets. This should provide you with a foundation to assess which roles have a higher risk of exposure, and may require additional employment checks.

As you recruit more people it is important to conduct additional screening of potential candidates who wish to be part of your business and have access to your information and assets. A suitable level of due diligence, informed by a role-based risk assessment, should be applied to individuals who are given access.

03
Case study

Some foreign states use think tanks as a way to collect intelligence or carry out influence operations. In one case, an overseas think tank, controlled by a foreign government set up office in New Zealand and held events promoting technology exchange and facilitating foreign investment in tech projects. While seeming to promote collaboration and investment the think tank also became involved in an organisation known to conduct foreign interference and which likely responds to the state's direction.

5.5 PRE-EMPLOYMENT CHECKLIST

Security checks which are part of your pre-employment due diligence could include:

- ✓ **Confirmation of Identity**
- ✓ **Nationality and immigration status**
- ✓ **Right to work in New Zealand**
- ✓ **Education and employment history**
- ✓ **Financial records**
- ✓ **Criminal records**
- ✓ **Personal references**
- ✓ **Open-source media** (including social media)
- ✓ **Eligibility for a national security clearance** (if they are accessing government classified material)

Further information

Learn more about growing your team:

- Insider threat risks – understanding the risk people pose to your organisation – *Protective Security Requirements*

5.6 INCIDENT MANAGEMENT

Incidents such as cyber attacks or other security breaches can happen at any point in your company's growth.

Damage caused by a security breach can be minimised through a well-planned and executed response. Assume your business will be breached and plan accordingly.

A basic incident management plan should include:

- contact details for anyone you would need to help you identify an incident
- clearly defined responsibilities and an escalation process for critical decisions
- a coordination function to track and document fundings and actions
- a mechanism to learn from previous incidents.

Think about:

- obligations you may have to report certain incidents to any relevant regulatory bodies.
- any risk or vulnerabilities in your systems so you can collect the right information to spot irregularities.
- what might cause uncharacteristic behaviour in your team that might lead to an insider threat (such as conflict at work, change in behaviour, or decline in performance). A supportive response may help mitigate risk, improve relationships, and build a positive security culture.

Further information

Learn more about managing incidents:

+ Reporting incidents and conducting security investigations – understand how to report, manage, and investigate security incidents using a consistent, structured approach – *Protective Security Requirements*
+ Incident Management: Be Resilient, Be Prepared – five key steps to help business leaders and security professionals manage cyber security incidents – *National Cyber Security Centre*

5.7 SECURITY CULTURE

Security culture is the set of values shared by everyone in your organisation that determine how people are expected to think about and approach security.

Consistency and communication are vital to creating an environment in which people are confident that they can speak openly about security concerns, that the organisation will improve as a result, and that any actions will be reviewed fairly. This means making it easy and routine to report any concerns, handling those concerns sensitively and without apportioning blame, and keeping those involved informed of both the progress and benefits of any resulting actions to reinforce confidence in reporting.

Everyone has a role to play. A sign of a strong security culture is when each member of the organisation knows their responsibilities and what is at stake.

RESOURCES

There is a range of advice available across the New Zealand government to support the tech sector to secure your innovation.

NZSIS and Protective Security Requirements

- New Zealand's Security Threat Environment 2024: an assessment by the New Zealand Security Intelligence Service
- Kia mataara ki ngā tohu – Know the signs: a guide for identifying signs of violent extremism
- Due Diligence for espionage and foreign interference threats
- Trusted Research: guidance for institutions and researchers
- Espionage and Foreign Interference Threats: security advice for members of the New Zealand Parliament and Locally Elected Representatives
- Managing Inwards Visits: protective security guidance
- Security Advice for New Zealand Government Officials travelling overseas on business
- **Trusted Business**: protective security guidance for New Zealand businesses[4]
- **Protective Security Threat and Risk guidance**: supporting New Zealand government organisations to effectively manage threats and risks[4]

National Cyber Security Centre

- NCSC Cyber Threat Report
- Charting Your Course: Cyber Security Governance
- NCSC Cyber Security Framework
- Business online security assessment tool
- Cyber Security Investment: A Structured Approach
- Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default
- Secure by Design: Choosing Secure and Verifiable Technologies
- Supply Chain Cyber Security: In Safe Hands
- Cyber security guidance for high-profile individuals
- Incident Management: Be Resilient, Be Prepared
- Lawful access to official data offshore

[4] Available November 2024

New Zealand Trade and Enterprise

- Intellectual property protection for NZ businesses
- Using reciprocal confidentiality agreements

Ministry of Foreign Affairs and Trade

- New Zealand's export controls regime
- New Zealand Strategic Good List
- Official advice for New Zealanders living and travelling overseas

Land Information New Zealand

- Overseas investment Guidance
- Notify your transaction

Protective Security Requirements (PSR)

The Protective Security Requirements (PSR) is part of the New Zealand Security Intelligence Service. It is the New Zealand government's best practice security policy framework for security governance as well as for personnel, information, and physical security. It is a tool that organisations can use to protect what matters and manage security effectively.

The PSR takes a risk-based approach designed for flexible implementation by any organisation to protect its people, information, and assets.

More information can be found at www.protectivesecurity.govt.nz

National Cyber Security Centre (NCSC)

The National Cyber Security Centre (NCSC) is part of the Government Communications Security Bureau. Its mission is to protect Aotearoa New Zealand's wellbeing and prosperity through trusted cyber security services.

We work to enable the protection, wellbeing and prosperity of Aotearoa New Zealand by providing trusted cyber security services. NCSC's strategic objectives are to:

- Defend national security
- Raise cyber resilience
- Facilitate digital transformation.

NCSC fulfils its objectives through four functional activities: providing preventative advice, and deterring, detecting and disrupting the types of malicious cyber activity that could affect the country's national security and economic wellbeing.

More information can be found at www.ncsc.govt.nz

Te Rōpū Pārongo Tārehu o Aotearoa
New Zealand Intelligence Community