Australian Government
Australian Security Intelligence Organisation

ASIO

SECURE INNOVATION

Building security into the foundations of your enterprise will make your security more effective and less costly as your business grows.

1 **Know the threats**
Understand the threats to your business and innovation

2 **Secure your business environment**
Identify, assess and mitigate security risks to your business

3 **Secure your products**
Build security into the foundations of your products and protect your IP

4 **Secure your partnerships**
Understand who you are working with, what you are sharing and how you are protecting your innovation

5 **Secure your growth**
Ensure your security practices grow as your business does

Australia has long been a **nation of innovation** – from the electric drill to wi-fi, penicillin to Google Maps, the black box recorder to the refrigerator.

This record continues today with diverse research, from quantum computing to ending plastic pollution through infinite recycling.

The strength of Australian innovation also makes it a **target for espionage**. A range of bad-faith actors are looking to **steal innovative technology** for their own benefit, and to **Australia's commercial detriment**.

Secure Innovation offers **simple protective security advice** for emerging technology companies.

It can be implemented quickly to make meaningful improvements to security. Simple steps can make a major difference to **your commercial success**.

For more information, visit the 'Resources' tab on the ***ASIO website*** *(www.asio.gov.au) and* ***ASIO's Outreach portal*** *(www.asio.gov.au/outreach)*

Security advice for emerging technology companies

25-0027

1 KNOW THE THREATS

There are a range of entities that could pose a **threat to your business** and innovation:

Foreign powers – foreign governments and entities under their direction – looking to steal your technology, data and intellectual property (IP) to fast-track their technological capability.

Foreign powers can put the technology to military use, but often it is given to **favoured companies** to mass produce, offering them a major commercial advantage while undercutting and undermining the innovator.

Foreign powers can also use your technology to target, harm and repress their own people, which may cause your company reputational damage.

Foreign powers may also use a range of unofficial **proxies** to approach or target you. These can include criminal groups, shell companies, foreign investment funds, foreign universities or researchers.

2 SECURE YOUR BUSINESS ENVIRONMENT

The start-up phase is the perfect time to set the tone for your future security culture. Ongoing conversations about security are vital to **developing a culture in which security incidents are discussed openly** and learnt from. The key steps are:

- Select a **senior executive** responsible for considering the security implications of business decisions.
- Identify your business's **critical assets.** These can include your people, premises, products and services, as well as IP and intangible knowledge.
- **Build security into your environment.** Build barriers (physical or virtual) around critical assets and restrict access to those who need it.
- **Implement good IT security.** Enable your firewall and antivirus, use strong passwords and multi-factor authentication, and ensure devices and software are up-to-date and vulnerabilities are patched.

3 SECURE YOUR PRODUCTS

Securing your products and intellectual property is vital to ensuring your business's long-term viability:

- **Secure your products from the beginning.** Use Secure by Design and Secure by Default principles to address security problems at the root cause. This will ensure you create products your customers can trust, protecting your long-term reputation.
- **Identify and actively manage your IP.** Intellectual Asset (IA) and IP management strategies are essential for any business. Understand your assets to determine what you need to protect and the measures required to protect it in the countries you operate in.

4 SECURE YOUR PARTNERSHIPS

Partnerships can increase the number of external routes into your organisation, or to any information or data you hold. To help you collaborate safely, consider:

- **Why are you collaborating?** What outcomes do you need, what are the benefits a partner brings and any risks or red lines.
- **Who are you (really) working with?** Conduct due diligence on all prospective investors, suppliers and collaborators.
- **What are you sharing?** Be strategic about what you share with partners and when.

Bear in mind your early choice of partners – whether investors, customers or suppliers – may impact who is willing to do business with you later on.

5 SECURE YOUR GROWTH

Your security culture should grow with your company. The risks you face will change, for example, as you hire more staff, move to multiple premises or look for new investors. Review your security mitigations regularly to ensure they still adequately protect your business.

The key steps are:

- Manage **electronic device security** and **personnel security** when your staff travel overseas.
- **Understand how local laws could increase the threat to your business overseas.** National security laws in some countries allow the government to legally appropriate any data or information stored in or transmitted via that country.
- **Deliver regular security training for your staff.** Raise staff awareness about potential threats, demonstrate you value good security and ensure staff understand their responsibilities.
- **Implement pre-employment screening,** particularly for staff in higher risk roles.

CASE STUDY

An Australian technology company invented a world-leading product, which was a significant success. Suddenly, the company experienced a huge drop in sales and loss of income, but didn't know why. Months later, faulty products were returned to them for repair. While the products bore the company's brand, they contained inferior components and shoddy workmanship.

The company investigated, engaged with ASIO and ASD, and they pieced together what had happened: a year earlier, a company representative at an international defence industry fair was approached by an 'enthusiastic attendee' from a third country. She insisted on sharing some content with them via a USB. However, the USB contained malware that remotely exfiltrated sensitive company information, including the plans for their proprietary product.

It is highly likely the 'enthusiastic attendee' at the industry fair was actually working for a foreign intelligence service. The foreign government passed the stolen blueprints to a state-owned enterprise to mass-produce for its own profit – at Australia's expense.

Espionage and foreign interference can occur anywhere, but the threat from foreign powers and their proxies is greater when they have the 'home-ground advantage', with near unrestricted access to hotels, airports and communication networks.

Before you travel overseas, consider the value of the sensitive information you hold and store on your electronic devices. What would happen if it ended up in the wrong hands?

By limiting the information on your devices to the bare minimum, you reduce the potential damage to your business, including loss of sales and profit, if the device is compromised.