TAKE FIVE
Cybersecurity

theprojectlab

What are the risks?

The business risks that come with minimal, or no cyber security practices or processes in place are real. From a mild inconvenience to your IT department, through to loss of your customers' trust, and even your business.

Did you know?

- Your organisation has a **1 in 4** chance of experiencing a **data breach**
- **60%** of small and mid-sized businesses that are **hacked** go **out of business** within 6 months
- **61%** of businesses have been affected by **ransomware**
- **90%** of cyber attacks start with a **phishing email**; and
- **31%** of customers impacted by a breach **discontinued their relationship** with the organisation.

What can you do about it?

You can minimise the risk to your business by investing in cyber security in a range of ways. Understand the threat, raise awareness and change your culture. Protect your assets. Detect and contain the threat. Learn as you go, and plan for recovery.

This simple **five step process** will help you get started.

1. **Identify**
2. **Protect**
3. **Detect**
4. **Respond**
5. **Recover**

Identify

Understand the relationship between Cyber Security Risk and key assets, systems and information in your organisation.

Dependency groups:

- Digital Information (CRM, HR, IP, Financial etc.)
- Non-digital Information (Plans, Certificates, Statements etc.)
- Things other than information (Stock, Buildings, Vehicle etc.)

Ask yourself:

- Would our organisation function without these dependencies?
- Do I know who has responsibility the dependency? Does the person know?
- Does our organisation know the restoration priority for our dependencies? Is CRM more important than payroll?
- Understand the asset's value to your organisation—will the organisation pay $50 for information held in a ransom attack? Would the organisation pay $1m?
- Does our organisation have internal/external obligations? How do we manage this? Examples are obligations to the Privacy Act?

Activities include:

- Document core business functions, their dependencies and owners
- Understand the links between business objectives, people, systems, assets and data
- Understand Risk Tolerance in context to your dependencies

Protect

Enable investment in cyber security to mitigate business risk.

Examples of protection investments:

- Access Control, including monitoring
- Culture, awareness and training
- Information Management, Processes and Procedures
- Ongoing maintenance
- Technology

Ask yourself:

- Is investment mitigating risk relevant to the dependencies of the organisation?
- Who has, and should have access to the organisation's dependencies?
- Does our organisation's culture acknowledge the risk of cyber security? How mature is our cyber security culture?
- Do staff know how to identify SPAM, and know not to click on it? If it looked like a legitimate request to transfer money, would they do it?

Detect

Facilitate quick identification of cyber security events. Understand what is 'normal' behaviour for your organisation's dependencies.

Actions include:

- Logging and Reporting (All three dependency groups)
- Continuous Review
- Process Design

Ask yourself:

- Who accesses the things required to operate the organisation?
- Do we incorporate Fail Safes into our dependency processes (e.g. funds transfer)?
- Do we have monthly security reporting from our Firewall, Anti-Virus and other key technology?
- Do we collect log files, or equivalent information, from key assets? Are they reviewed?
- When was the last time we scanned every PC for threats? How often should this be done?

Respond

Contain the threat. Communicate. Retain the trust of your suppliers and customers.

Actions include:

- Have, document and maintain a plan
- Communicate the plan
- Plan for containment
- Learn from execution of the plan

Ask yourself:

- Work backwards — who is responsible, who owns the plan? Do we need approval (funds)? Who do we tell?
- Analyse the plan's requests and actions — have we ensured adequate actions are performed? Have we enabled ways to learn from execution of the plan?
- How do we prevent spread of the threat? How do we mitigate its effect and eradicate the incident?
- What did we learn from current and previous incidents?

Recover

Effectively restore the dependencies you need to operate the organisation. Work with external organisations that may have been affected. Learn from the process.

Actions include:

- Business Continuity Planning, allocate ownership
- Testing Plans
- Lessons Learned, look for improvements
- Communication

Ask yourself:

- What is our Business Continuity plan?
- How can we incorporate lessons learned into Recovery plans?
- Have we communicated to relevant internal and external parties? Remember — your priorities will dictate recovery — communicate your 'what' and 'when' clearly.

Action points

Cyber attacks are serious threats to all organisations. While technology plays a part in risk mitigation and protection, it's the business that owns and manages the risk.

- Start the cyber security conversation in your organisation
- Put a team together to own, implement and maintain your response to cyber security risk
- Consider the legal obligations and privacy laws that apply to Australian business entities
- Understand the five steps, get informed and protect your organisation

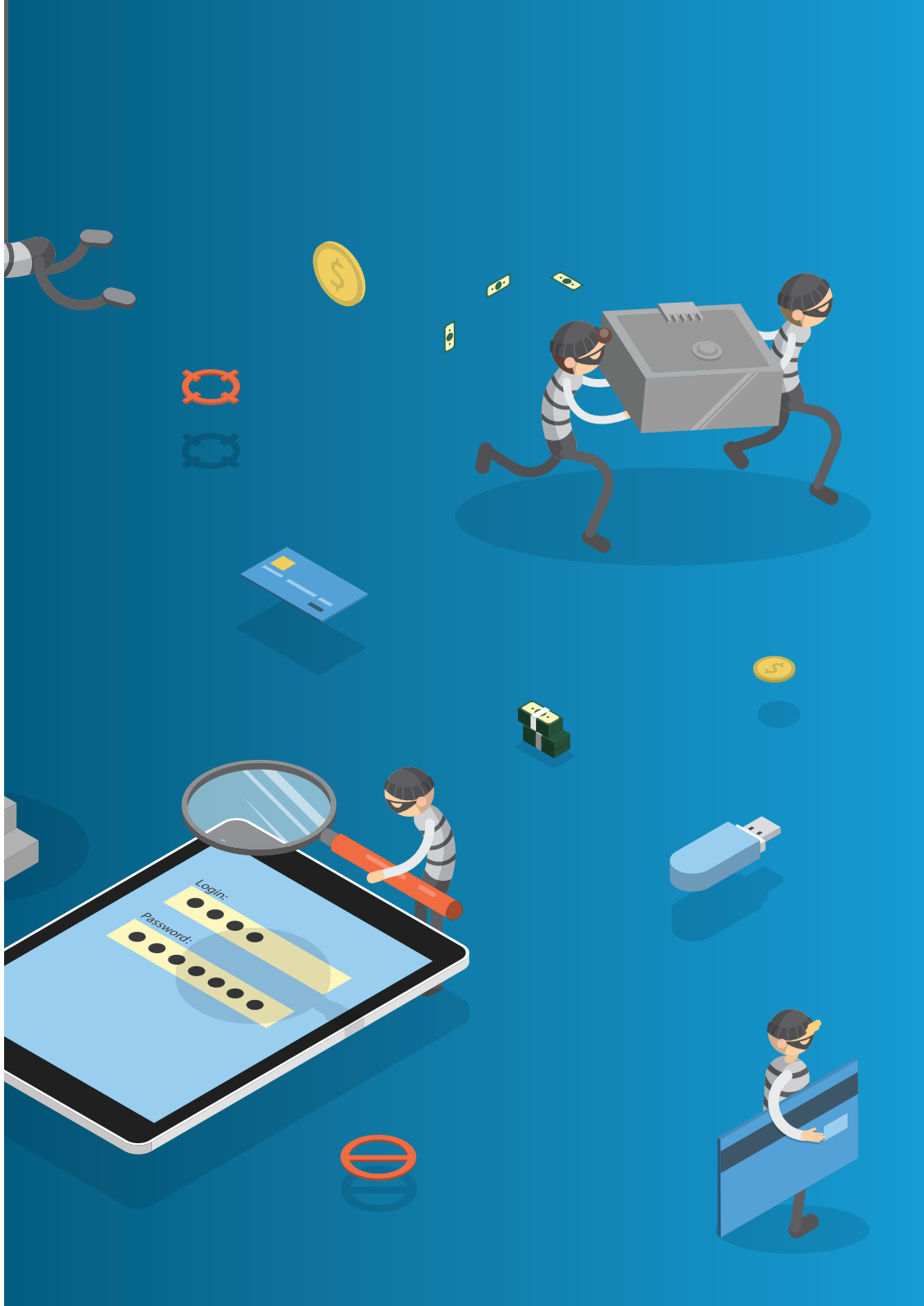
You're not alone

Our consultants have years of experience working with Australian businesses to successfully manage and mitigate cyber security risk.

We provide cyber security risk advisory services and insurance, and can help your business identify vulnerabilities and inconsistencies.

If you're concerned about cyber security readiness, need guidance on protecting your business from cyber threats, or simply want to understand the fundamental risks, we can help.

Contact the team at Project Lab for more information.



theprojectlab

The Project Lab is a boutique consultancy & advisory firm that specialises in providing organisations with qualified and highly experienced people.

For more information please contact us to arrange a meeting.

take5@theprojectlab.com

1300 843 776