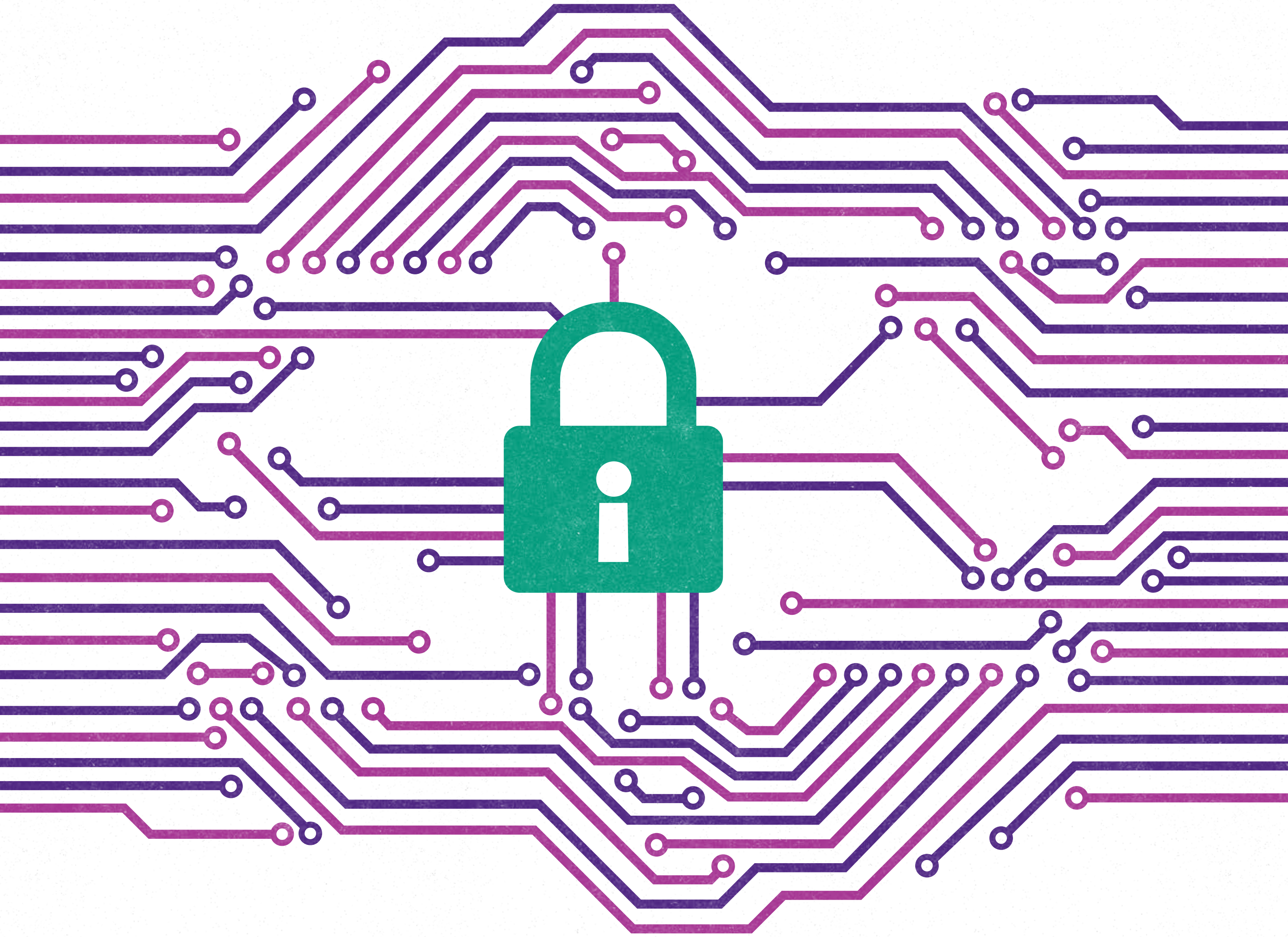
Grant Thornton

An instinct for growth™

How to be cyber secure

A practical guide for Australia's mid-size business



Introduction

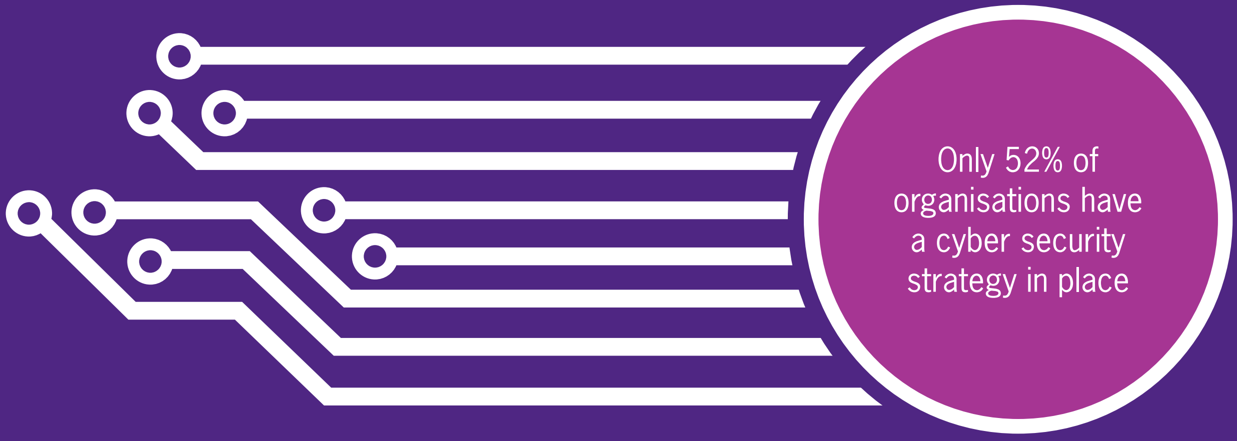
The digital age has bred opportunity for mid-size business. From ecommerce to social media, agile organisations have taken advantage of new channels to disrupt their industries and fuel rapid growth. However, technology developments have also introduced new risks. Rated a top 10 global exposure both likelihood and severity-wise by the World Economic Forum, cyber risk is now a top level agenda item for boards worldwide.

Cyber risk is here to stay, but not necessarily in its current form. While businesses worry about data privacy and IP theft today, they may well face different conundrums tomorrow. The internet of things is widening the scope of cyber attacks with its potential to inflict damage on infrastructure and mass production. Closer to home, the frequency of cryptolocker and ransomware attacks against Australian companies is on the rise, with a direct impact on organisations' operational fitness and bottom line.

While hackers are not shy about reinventing their way of working, business may not be as nimble when it comes to counteracting the threat: Grant Thornton's recent International Business Report (IBR) points out that only 52% of organisations have a cyber security strategy in place.

Not all companies are created equal when it comes to cyber risk. While equally vulnerable targets for cyber crime or hacktivism, mid-size businesses are generally less equipped to deal with the consequences of attacks than their multinational counterparts. The Australian government has recently acknowledged this gap, and launched the national Cyber Security Strategy, which directly addresses the need for cyber risk advice adapted to businesses of all sizes.

Grant Thornton, mid-size businesses' growth advisor of choice, accompanies a broad range of organisations in identifying cyber exposures, developing effective risk management strategies, implementing the necessary measures to safeguard operations, and acting swiftly to counteract and recover from potential attacks. We understand that mid-size businesses need a pragmatic and cost-effective approach to managing cyber risk; this is why our experts provide counsel and support adapted to each company's profile, and focus on delivering results.



Only 52% of organisations have a cyber security strategy in place

What does this mean to mid-size businesses in Australia?

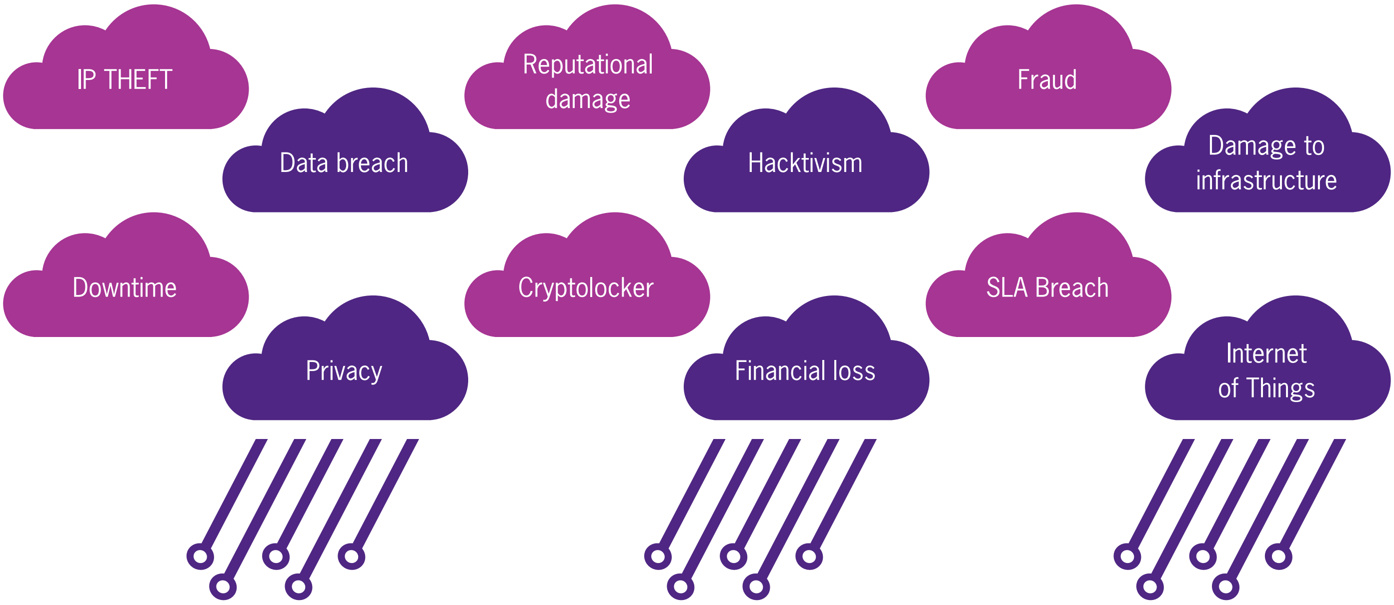
Cyber risk awareness is no longer enough. With Australia an increasingly attractive target for cyber crime, businesses need to act in order to prevent attacks, build resilience, and foster a culture of cyber security among their employees.

Furthermore, companies trading abroad need to take into account foreign legal and compliance requirements, as well as threats specific to each market they operate in. As governments around the world act to counter cyber risk, it is well to bear in mind that the legislative landscape is varied: ranging from sophisticated in Australia, the United States and Europe, to emerging across Asia, where few mandatory requirements to report breaches exist and cyber safety standards are patchy.

Mid-size businesses need robust cyber security policies in order to deal with this evolving exposure. Grant Thornton's cyber security experts have designed a practical guide to being cyber-secure for Australia's mid-size businesses.

> *Businesses need to act in order to prevent attacks, build resilience, and foster a culture of cyber security among their employees.*
>
> **Matthew Green**
> Partner, Grant Thornton Australia

What is cyber risk?



What can mid-size business do about cyber risk?

STEP 1: PREVENT

Conduct a risk assessment

The first step to preventing cyber attacks is to assess your company's exact risks: determine key assets and processes, pinpoint vulnerabilities, and identify areas of improvement. The risk assessment should focus not only on the current state of the organisation but also take into account its growth strategy, and the technological needs going forward. The goal of the risk assessment is not only to identify immediate action items, but also to provide visibility of potential exposures over the long term. In this way your organisation is supported to make well-informed decisions regarding future-state technology.

While a strategic outlook allows leaders to consider cyber risk in the broader business context, a technical security assessment is a critical step to securing business operations. Grant Thornton cyber experts conduct a full cyber security assessment including:

- Cyber security risk and governance assessment
- External vulnerability assessment and penetration testing.
- Internal vulnerability assessment and penetration testing.
- Web application vulnerability assessment.
- Wireless networks vulnerability assessment.
- Security configuration assessments.

Our six-step assessment methodology allows us to present businesses with a detailed report of cyber risk management, potential vulnerabilities, and make recommendations for improving cyber security.

Create a robust cyber security policy

The risk assessment results should be integrated into a robust, organisation-wide cyber security policy that focuses on people, processes and technology.

- **Make smart technology choices** – 'Privacy by design' is becoming increasingly embedded in IT platforms worldwide; however, companies should also pay attention to 'security by design'.
- **Apply strict criteria to vendor selection** – Compliance with cyber security norms, as well as recovery planning and support, are key criteria for IT vendor selection. Mid-size businesses seeking cost-efficiency when buying technology should not sacrifice safety.
- **Build a cyber-secure culture** – Building a cyber-secure culture is perhaps the broadest area of development for businesses. From social media policies to cyber security training, companies need to create awareness and foster the right behaviours among their people.

Continuously monitor your IT infrastructure and processes

Once a cyber security policy is in place, continual monitoring and training is required for optimal results. Vigilance and proactivity are the best types of prevention.

STEP 2: REACT

However, track records so far indicate that most companies will experience a cyber security incident at one point in time. What can organisations do in case of a cyber attack?

Quick reaction

It is important that businesses react quickly in case of a cyber incident, and follow a strict protocol in controlling damage both internally and externally. Cyber security policies should include a clear outline of measures and of resources available in case of an incident.

Crisis management

Critical points related to crisis management should be outlined in the cyber security strategy, along with action owners and available resources to manage the deployment of internal measures and handle external queries.

Incident handling process

When a cyber incident does occur, it is important to follow a step-by-step approach. When working with our clients Grant Thornton cyber experts apply the following process:

1. Identification
Ascertaining the exact nature and extent of the incident is critical to managing it properly going forward.

2. Validation and assessment
The assessment phase allows us to qualify the incident in terms of gravity and potential long-term impact.

3. Preliminary report
A first report is delivered, outlining the issue and proposing pragmatic solutions.

4. Containment
Once a decision is made regarding the strategy, we proceed to containing the incident, and to preventing any further damage.

5. Eradication
Once the immediate fire is put out, it is important to check the overall health of the system, and ensure that no further threats are present.

STEP 3: RECOVER

Recovery plan

The growing diversity of cyber incidents requires swift reaction. Robust systems and responsive technology providers, along with a good crisis management team, can make the difference in safeguarding investments and reputation, and recovering successfully.

When recovering from a cyber incident, it is important to conduct further testing to make sure all systems are functioning perfectly, and to monitor operations for a period of time, like a post-surgery patient.

Safeguard reputation

Businesses that have experienced cyber incidents agree: reputation is one of the most sensitive areas affected by an attack, and among the most difficult to fix. Organisations must put in place brand remediation measures within the crisis management phase, and focus efforts on clear and coherent communication throughout the process.

As cyber attacks increase in number and severity businesses need to build defences, implement security strategies and foster risk-aware cultures. The end goal: a cyber-resilient business focused on sustainable growth.

Cyber security checklist

STEP 1: PREVENT

Conduct a cyber risk assessment

- □ **Strategic considerations**
- □ **Technical security assessment**
  - □ Internal and external vulnerability assessment and penetration testing
  - □ Web application, wireless network, PBS and VOIP assessment
  - □ Security configuration assessment

Create a robust cyber security policy

- □ Technology choices
- □ Vendor selection
- □ Cyber-secure cultures

Build a resilient IT governance framework

STEP 2: REACT

Quick reaction

Crisis management

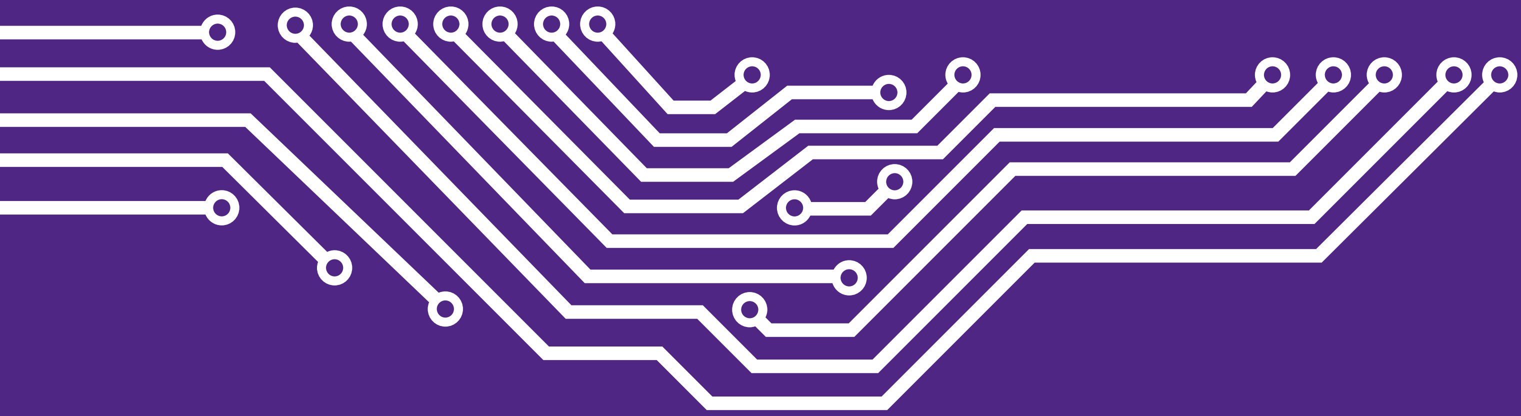
Incident handling process:

- □ Identification
- □ Validation and assessment
- □ Preliminary report
- □ Containment
- □ Eradication

STEP 3: RECOVER

Recovery plan and testing

Safeguard reputation



Our services

Grant Thornton Technology Advisory and Solutions supports mid-size businesses, not for profit organisations and government agencies throughout their digital transformation journeys. We effectively act as an innovation partner: we support organisations to develop, implement and review technology strategies, systems and processes aligned with their business goals.

Our specialists work with clients across the globe to help them understand and respond to cyber-security threats to their organisation. As well has assessing risk and helping to improve cultures, technologies and processes, our people help organisations identify, respond to and investigate cyber-security incidents and breaches.

Grant Thornton is one of the world's leading organisations of independent assurance, tax and advisory firms. These firms help dynamic organisations unlock their potential for growth by providing meaningful, forward looking advice. Proactive teams, led by approachable partners in these firms, use insights, experience and instinct to understand complex issues for privately owned, publicly listed and public sector clients and help them to find solutions. Grant Thornton Australia has more than 1,000 people working in Adelaide, Brisbane, Cairns, the Gold Coast, Melbourne, Perth and Sydney. We combine service breadth, depth of expertise and industry insight with an approachable 'client first' mindset and a broad commercial perspective.

Contact

Alex Gelman
Partner & National Head of Technology Advisory & Solutions
T +61 2 8297 2422
E alex.gelman@au.gt.com

Robert Samuel
Partner – Technology Advisory & Solutions
T +61 2 8297 2429
E robert.samuel@au.gt.com

Matthew Green
Partner – Technology Advisory & Solutions
T +61 3 8663 6168
E matthew.green@au.gt.com

John Picot
Principal – Technology Advisory & Solutions
T +61 2 8297 2426
E john.picot@au.gt.com

Grant Thornton
An instinct for growth™

www.grantthornton.com.au

Grant Thornton Australia Limited ABN 41 127 556 389 ACN 127 556 389

'Grant Thornton' refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires. Grant Thornton Australia Ltd is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate one another and are not liable for one another's acts or omissions. In the Australian context only, the use of the term 'Grant Thornton' may refer to Grant Thornton Australia Limited ABN 41 127 556 389 and its Australian subsidiaries and related entities. GTIL is not an Australian related entity to Grant Thornton Australia Limited.

Liability limited by a scheme approved under Professional Standards Legislation. Liability is limited in those States where a current scheme applies.

EPI.147.16