SECURITY OF CRITICAL INFRASTRUCTURE SOLUTIONS

RISK 2 SOLUTION GROUP

2022

WWW.RISK2SOLUTION.COM

PROTECTING WHAT COUNTS.

We work with you as a partner to assure robust and balanced strategies that deliver peace of mind to you. We are here to help you “Protect What Counts” by securing your property, business, and people. Our robust Physical Security and Consulting services can support you and your business with the following services.

Introduction to **Security of Critical Infrastructure (SoCI)**

In early 2022, the Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 was passed by the Australian Parliament to amend the 2018 SoCI (Security of Critical Infrastructure) Act. This Act expands the sectors considered as CI (Critical Infrastructure) to include:

- ✓ Communications
- ✓ Data storage or processing
- ✓ Higher education & research
- ✓ Food & grocery
- ✓ Space technology
- ✓ Water & sewerage
- ✓ Financial services & markets
- ✓ Defence industry
- ✓ Energy
- ✓ Health care & medical
- ✓ Transport

One of the major catalysts for this expansion was a substantial increase in cyber-attacks, with the United Nations reporting a 600% increase. Perhaps the most sobering aspect of these attacks is that 25% were aimed at CI organisations, with the Global Risk Report 2022 by the World Economic Forum concluding that Australia's number one risk concern is "Failure of Cyber Security Measures".

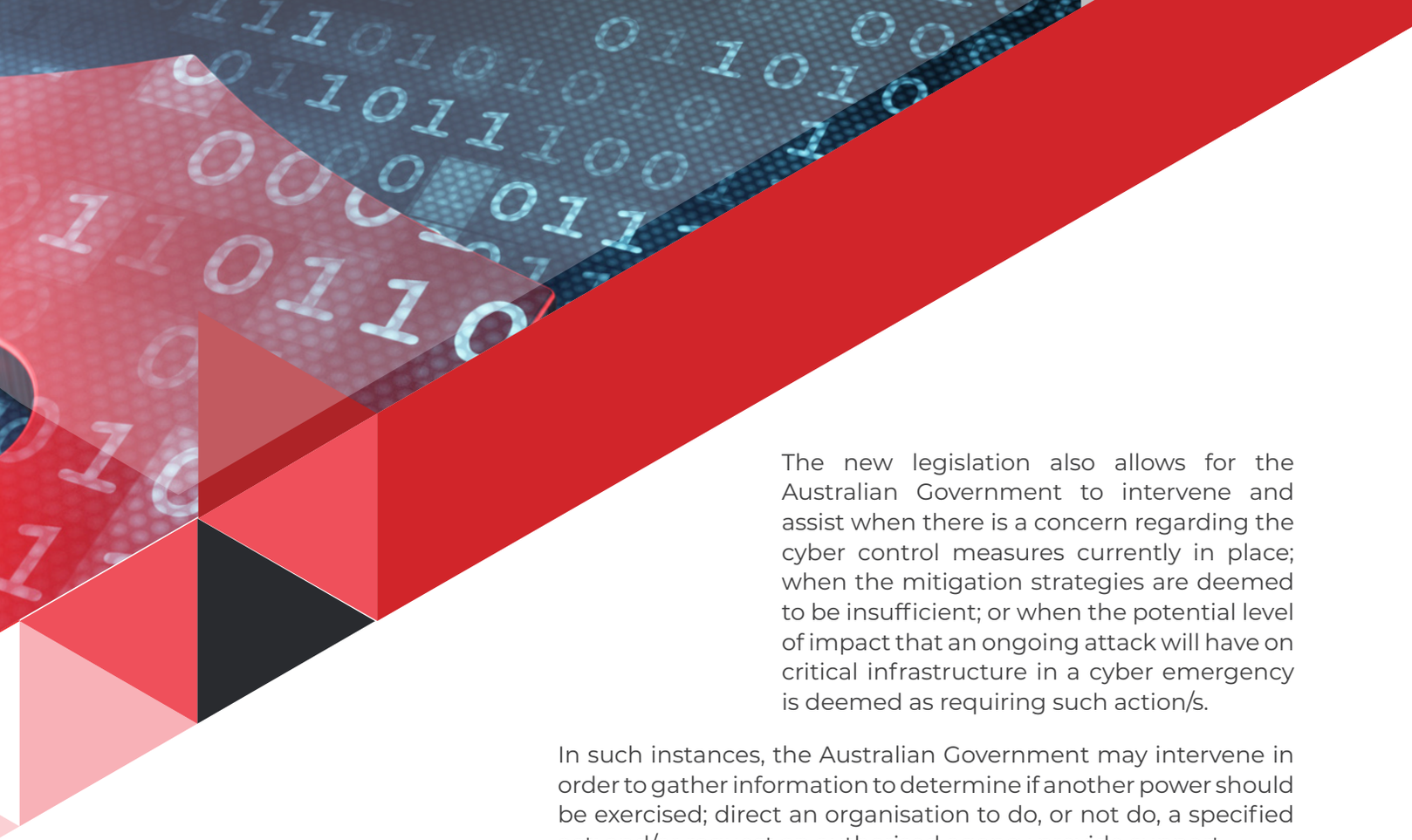
RISK 2 SOLUTION
PROTECTING WHAT COUNTS

WHAT DOES THE **UPDATED LEGISLATION** MEAN?

Under the new legislation, there are enhanced cyber security obligations whereby organisations will need to establish processes for incident response, regular cyber security test exercises, vulnerability management, and to be able to provide security incident reporting on-demand.

✓ **The implementation of this new legislation carries with it some substantial challenges, with the requirements including:**

- registration of critical assets: identification, classification, and accountability
- common understanding or risk-based and protective security
- effective risk management framework by sector, with common measurements and assessments
- communication between Home Affairs, state governments, and other stakeholders
- governance
- definition and parameters of scope of Ministerial Controls (Cyber)
- communication in a national security context
- mandatory reporting of cyber issues
- transparency requirements for the CI Owners: Reporting requirements, Cyber intervention, Government intervention in cyber-attack/s



The new legislation also allows for the Australian Government to intervene and assist when there is a concern regarding the cyber control measures currently in place; when the mitigation strategies are deemed to be insufficient; or when the potential level of impact that an ongoing attack will have on critical infrastructure in a cyber emergency is deemed as requiring such action/s.

In such instances, the Australian Government may intervene in order to gather information to determine if another power should be exercised; direct an organisation to do, or not do, a specified act; and/or request an authorised agency provide support.

Other obligations under the SoCI legislation include Positive Security Obligations (PSO), which involve the accountability for the security of critical assets, data security measures, and notification timeframes for cyber incident reporting.

THE **"FOUR PILLARS"**

The new legislation is comprehensive, and will focus on four pillars of security, namely:

1

Cyber and Information Security

It is vitally important for organisations, critical infrastructure and otherwise, and the ongoing cooperation between the Australian Government and the private sector is crucial to maintain the security of our networks and systems.

2

Personnel Security

It is needed to ensure that existing and new staff who will have access to systems and data are properly vetted, and that an increased sense of risk awareness and a positive risk mindset/culture is worked towards.

3

Physical Security

Needs to find the balance between restricting access to assets and critical infrastructure by unauthorised persons with the need for operational access by authorised personnel, efficient user interface, and environment protection.

4

Supply Chain & Business Continuity Security

Requires critical infrastructure organisations to actively manage their supply chain and business continuity security risk exposures in order to ensure their ongoing ability to meet their obligations for service provision.

WHY R2S

Risk 2 Solution is Australia's most awarded integrated risk experts. We pride ourselves on offering a holistic suite of services to address tactical, operational and strategic risks for our clients that is unmatched by any other Australian provider. Through the strength of our group of companies, we are uniquely positioned to provide truly integrated solutions to the complex challenges of enterprise security in 2022 and beyond.

Some of our recent awards include:

- ✓ 2021 AFRBoss Top 10 Most Innovative Professional Services firm in Australia
- ✓ Outstanding Security Consultant of the Year 2021
- ✓ RMIA Risk Consultant of the Year 2019
- ✓ Only company in the world to feature two members on the prestigious IFSEC Global Top Influencers in Security list in 2022
- ✓ Group CEO Gav Schneider the only Australian to feature on the IFSEC Global Top Influencer list for four consecutive years (2019-2022)

We have provided integrated physical security advisory and protective security solutions for clients throughout Australia and internationally – providing a holistic approach that encompasses risk management, physical security, personnel security, cyber security and supply chain management. We have a track record of providing high level security and risk services for several major critical infrastructure entities. References are available upon request.

HOW WE CAN HELP

- Comprehensive risk management services including program design, risk culture uplift and strategic implementation of risk treatments
- Cyber security maturity assessments leveraging our exclusive partnership with AXIO 360 – the US's leading critical infrastructure cyber specialists
- Domain Vulnerability and Penetration Testing
- Cyber security education, response and uplift
- Physical security design
- Security risk assessments and site audits
- Open source intelligence and investigations
- Personnel security audits and system design
- Occupational violence and aggression management
- Supply chain audit and analysis

100+
Years experience in management team

500+
Successfull consulting engagements

30+
Countries operated in

INTEGRATION AND TURNKEY SOLUTIONS

R2S is Australia's most awarded integrated risk business that has the capability, maturity, countrywide footprint, and experience to work with you to mature, validate and project manage your Security journey.

CONTACT US

To discuss how R2S can help your business *Protect What Counts*, please contact:

Dave Cohen
Group Head of
Business Development
E dave.c@risk2solution.com
M +61 493 087 729

Some of the key organisations we have worked with:

ActewAGL

Australian Government
Department of Foreign Affairs and Trade

Australian Government
Department of Defence

NSW GOVERNMENT Transport

CSIRO

Australian Government
Services Australia

Bendigo TAFE

KANGAN INSTITUTE

ACU
AUSTRALIAN CATHOLIC UNIVERSITY

IBA INDIGENOUS BUSINESS AUSTRALIA

AMP CAPITAL

icare

CITY OF GOLD COAST.