/ CLOUD CONTROL /

# ADC

THE NEXT GENERATION DATA CENTRE

# PROTECTING AUSTRALIA'S DATA IN THE NEW CYBER WORLD ORDER – A WHITEPAPER

WWW.AUSDATACENTRE.COM.AU

# Contents

# PROTECTING AUSTRALIA'S INTERESTS

The data contained within Australia's national critical infrastructure is of such consequence it underpins the functioning of our society and the economy. It is integral to the prosperity of the nation.

In recent years, however, concerns have grown about the threat posed by malevolent cyber interests. So too has our awareness of the significant costs inherent in any loss, interruption or damage to the systems we rely on.

The danger is escalating, with greed, geo-political tensions and the sinister capabilities of hackers leading to the infiltration of some essential systems that had been considered impermeable.

> *National Critical Infrastructure is defined as 'those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security'.*

In June 2020, Prime Minister Scott Morrison confirmed that Australian entities were "being targeted by a sophisticated state-based cyber actor" in what was a startling attack on our national interests.

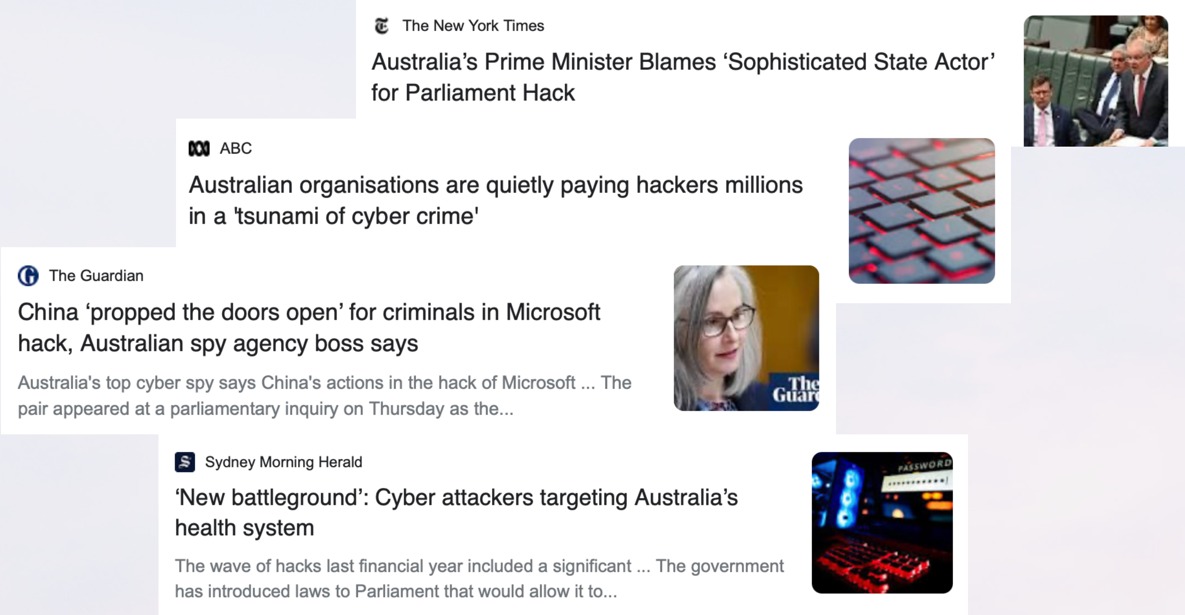
"This activity is targeting Australian organisations across a range of sectors, including all levels of government, industry, political organisations, education, health, essential service providers, and operators of other critical infrastructure," Mr Morrison said.

"We know it is a sophisticated state-based cyber actor because of the scale and nature of the targeting and the tradecraft used."

In September last year, Defence Minister Linda Reynolds described a "new normal" of unrelenting cyber attacks on the nation.

"We're now facing an environment where cyber-enabled activities have the potential to drive disinformation, and also directly support interference in our economy, interference in our political system, and also in what we see as critical infrastructure," Senator Reynolds said.

"This type of activity really does blur what we previously understood to be peace and war, which is what we call that grey zone in between."



The New York Times

Australia's Prime Minister Blames 'Sophisticated State Actor' for Parliament Hack

ABC

Australian organisations are quietly paying hackers millions in a 'tsunami of cyber crime'

The Guardian

China 'propped the doors open' for criminals in Microsoft hack, Australian spy agency boss says

Australia's top cyber spy says China's actions in the hack of Microsoft ... The pair appeared at a parliamentary inquiry on Thursday as the...

Sydney Morning Herald

'New battleground': Cyber attackers targeting Australia's health system

The wave of hacks last financial year included a significant ... The government has introduced laws to Parliament that would allow it to...

The rhetoric may appear dramatic but cyber attacks on Australian systems have serious implications, and some of them go far beyond the financial or reputational.

The Australian Cyber Security Centre reported in September 2021 of "significant targeting, both domestically and globally, of essential services", which had "underscored the vulnerability of critical infrastructure to significant disruption in essential services, lost revenue and the potential of harm or loss of life".

Given the potential impacts, the statistics are alarming. Ransomware attacks disclosed to the ACSC increased 15 per cent in the 2020-21 financial year, with more than 67,500 reports of cybercrime of all types reported: or one every eight minutes.

Around one quarter of incidents affected critical infrastructure organisations, including education, health, communications, electricity, water and transport. In 14 cases, federal government entities or nationally significant infrastructure suffered the removal or damage of sensitive data or intellectual property.

***More than $33 billion was lost by business, individuals and other entities during 2020-21 due to cyber crime.***

Among the high profile attacks in Australia have been hacks on federal parliament, the Australian National University, the Nine Network, transport and logistics giant Toll Group and a Victorian public health service comprised of four hospitals and aged care facilities that was forced to postpone surgeries.

The consequences of each have been significant.

# A CYBER WAR FOOTING

The heightened level of concern has led the Commonwealth Government to take significant steps to ensure the cyber security of Australia's national critical infrastructure.

- The Security Legislation Amendment (Critical Infrastructure) Bill was introduced into Parliament on 10 December 2020 and expanded the scope of the 2018 Act to include a wider range of sectors including: "communications; financial services and markets; data storage or processing; defence industry; higher education and research; energy; food and grocery; health care and medical; space technology; transport; and water and sewerage".

- To ensure Australian data remains uncompromised by foreign actors, the Foreign Investment Reform (Protecting Australia's National Security) Act 2020 and the Foreign Investment Reform (Protecting Australia's National Security) Regulations 2020 have assigned a national security test for foreign investments to minimise risk.

- The Digital Transformation Agency has instituted a Whole-of-government Hosting Strategy which classifies data centres according to their sovereignty and the degree of certainty of their ownership and control by Australian shareholders.

- The Government Hosting Certification Framework works in conjunction with the powers and provisions of the Government's 2020 Cyber Security Strategy, including those relating to protecting critical infrastructure and systems of national significance.

- The Ransomware Action Plan will see the introduction of mandatory reporting of all ransomware incidents to the Australian Government.

These initiatives are crucial in order to keep Australians' data safe but they have placed numerous additional regulatory requirements on government, not-for-profit and commercial entities, including penalties for failure to comply.

> Between 2011 and 2020 the total amount of data created, captured, copied and consumed in the world grew from 2 to 64.2 zettabytes. In 2025, it is expected to skyrocket to 181 zettabytes.

# THE NEW OIL

In 2017, The Economist made a bold claim in a headline: "The world's most valuable resource is no longer oil, but data."

Such is its importance, every industry has been transformed by digital technologies and, as a result, oceans of data are being continually collected.

“The generation and use of vast amounts of data is a new source of market power in the digital economy,” according to the Department of Industry, Science, Energy and Resources.

“Data is a key economic commodity that can make existing businesses more efficient and is driving new business models and industries. Data-driven businesses can now easily access powerful data analytics to gain valuable insights about their customers or potential markets which can help them grow.”

Data also allows governments to deliver social benefits by providing services that are targeted and effective thanks to the insights gained through analysis of the troves of information.

So valuable is data that Australia’s digital economy is driving the nation’s economic recovery from the COVID-19 pandemic, with a new Australian Data Strategy designed to supercharge innovation via improved data access, sharing and asset management.

Within the strategy, the federal government is investing $111.3 million to support the acceleration of the Consumer Data Right rollout, $40.2 million to deliver a digital atlas of the nation, and $16.5 million for a pilot to create a Government Data Catalogue and allow whole-of-economy access to the Australian Government's considerable data assets.

*“It is a capital mistake to theorise before one has data.”*
*~ Sherlock Holmes, 1887,* A Study in Scarlet, *Arthur Conan Doyle*

The massive shift to digital platforms – and acceptance of them – as a result of the COVID-19 pandemic has certainly accelerated the **Fourth Industrial Revolution**.

So significant has the change been, the McKinsey Global Institute has claimed the "next normal" will affect the global economy and change society: "... just as the terms 'prewar' and 'postwar' are commonly used to describe the 20th century, generations to come will likely discuss the pre-COVID-19 and post-COVID-19 eras."

A McKinsey survey published in October 2020 found that companies were three times more likely than they were before the crisis to conduct at least 80 per cent of their customer interactions digitally.

"There's no going back. The great acceleration in the use of technology, digitisation and new forms of working is going to be sustained. Many executives reported that they moved 20 to 25 times faster than they thought possible on things like building supply-chain redundancies, improving data security and increasing the use of advanced technologies in operations."

As a result of this rapid tech uptake, between 2011 and 2020 the total amount of data created, captured, copied and consumed in the world grew from 2 to 64.2 zettabytes. In 2025, it is expected to skyrocket to 181 zettabytes.

And within the vast volumes of the data being collected are insights. For organisations, those insights can highlight consumer behaviours, market trends, productivity, performance and efficiencies.

Companies that adopt data-driven decision making achieve 5 to 6 per cent higher productivity and output growth than their competitors, according to the director of the Stanford Digital Economy Lab, Erik Brynjolfsson. Similar benefits were found in return on investment and market value.

The advantages, therefore, are substantial.

# IN SAFE HANDS

The custodians of sensitive data have responsibilities to protect the security, privacy and confidentiality of Australians' valuable information. They need to ensure it is stored in fortified data vaults that adhere to our new, complex regulatory regime.

Australian Data Centres removes the burden from national critical infrastructure organisations by providing the highest level of cybersecurity and data management capabilities from a world class facility in Canberra.

- ✓ Securing Australia's critical data where it needs to be – in Australia
- ✓ 100 per cent Australian owned and managed digital infrastructure
- ✓ Advancing Australia's technological capability, resilience and cybersecurity
- ✓ Multi-cloud enabled data facilities
- ✓ Disrupting the cloud market to reinvent the way it operates
- ✓ Providing simplified access to the world's best digital services.

Australian Data Centres is a private and wholly owned and operated Australian company that hosts Commonwealth department tenants and their gateways, as well as Australian international telecommunications companies and commercial organisations.

A **Certified Strategic** data centre, ADC provides a highly secure and independently certified **Tier III** data centre (Uptime Institute) with **no single point of failure** and efficiencies built into all levels of its technical design and implementation.

# THE SKY'S THE LIMIT

The global COVID pandemic has accelerated the uptake of cloud services, with the market expected to more than double in the next 5 years to USD$832.1 billion.

The availability of essentially unlimited compute power on demand has led organisations to look to the cloud, with cost benefits, scale, consumption-based pricing and access to new technologies and services, as well as better security, resiliency and enterprise-grade capability also on offer.

ADC’s cloud-enabled data centre model meets the imperative for supply chain certainty, Australian ownership, enhanced cybersecurity and access to multiple private and public clouds.

A multicloud strategy can allow organisations to take advantage of cost savings and innovations across providers. ADC acts as the conduit to the cloud providers.

Australian Data Centres provides technology choice, operational agility and financial governance across multiple cloud providers, with a focus on simplified consumption, deployment, security assurance and management.

With hybrid and multicloud offerings tailored to organisations' unique needs, co-location and connectivity to new and existing infrastructure, can also include private, as well as sovereign, cloud infrastructure.

All of this is provided within a state-of-the-art Certified Strategic facility in Canberra.

Because at ADC, data is recognised as the oil that – via our national critical infrastructure – fuels government, industries and the economy.

ADC

WWW.AUSDATACENTRE.COM.AU

# REFERENCES

Page 3

Prime Minister The Hon Scott Morrison MP, Statement on malicious cyber activity  against Australian networks, https://www.pm.gov.au/media/statement-malicious-cyber-activity-against-australian-networks

Cyber attacks on Australia blurring the lines between peace and war, Defence Minister says, https://www.abc.net.au/news/2020-09-04/cyber-attacks-on-australia-peace-war-defence-minister/12626396

Page 4

ACSC Annual Cyber Threat Report 2020-21, https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21

Exclusive: Australia concluded China was behind hack on parliament, political parties – sources, https://www.reuters.com/article/us-australia-china-cyber-exclusive-idUSKBN1W00VF

ANU releases detailed account of data breach, https://www.anu.edu.au/news/all-news/anu-releases-detailed-account-of-data-breach

Why was Nine hacked and how do cyber attacks actually work?, https://www.smh.com.au/national/why-was-nine-hacked-and-how-do-cyber-attacks-actually-work-20210329-p57ewm.html

Toll concedes it may not have worked with cyber spy agency fast enough during major hack,https://www.smh.com.au/politics/federal/toll-concedes-may-not-have-worked-with-australia-s-cyber-spy-agency-fast-enough-during-major-hack-20210802-p58f59.html

Staff unable to access patient files after Eastern Health cyber attack, https://www.theage.com.au/national/victoria/staff-unable-to-access-patient-files-after-eastern-health-cyber-attack-20210329-p57eyj.html

Page 5

Security Legislation Amendment (Critical Infrastructure) Bill 2021, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6657

Foreign Investment Reform (Protecting Australia's National Security) Act 2020, https://www.legislation.gov.au/Details/C2020A00114

Foreign Investment Reform (Protecting Australia's National Security) Regulations 2020, https://www.legislation.gov.au/Details/F2020L01568

Whole-of-Government Hosting Strategy, https://www.dta.gov.au/our-projects/whole-government-hosting-strategy

Hosting Certification Framework, https://www.dta.gov.au/our-projects/hosting-strategy/hosting-certification-framework

Australia's Cyber Security Strategy 2020, https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf

Protecting Critical Infrastructure and Systems of National Significance, Security Legislation Amendment (Critical Infrastructure) Bill 2020, https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-critical-infrastructure-systems

Ransomware Action Plan, https://www.homeaffairs.gov.au/cyber-security-subsite/files/ransomware-action-plan.pdf

Page 6

The world's most valuable resource is no longer oil, but data, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

What are the opportunities in data?, https://www.industry.gov.au/data-and-publications/australias-tech-future/data/what-are-the-opportunities-in-data

Australia's Digital Economy, https://digitaleconomy.pmc.gov.au/fact-sheets/data-and-digital-economy

Page 7

The next normal arrives: Trends that will define 2021—and beyond, https://www.mckinsey.com/featured-insights/leadership/the-next-normal-arrives-trends-that-will-define-2021-and-beyond

Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025, https://www.statista.com/statistics/871513/worldwide-data-created/

## CONTACT ADC

(02) 6185 0249
info@ausdatacentre.com.au
WWW.AUSDATACENTRE.COM.AU