media

Project:

CYBERSECURITY AUSTRALIA 2022

The resource guide of the latest information, products and services in the cybersecurity sector.

Media Kit

Welcome

Thank you for your interest in the 2022 editions of *Cybersecurity Australia,* the comprehensive resource guide of the latest information, products and services in the cybersecurity sector.

Cybersecurity is a high priority for Australia with cybercrime estimated to cost the country more than $1 billion every year. As the cyber threat landscape continues to evolve, sector revenue is forecast to continue to grow at about nine per cent each year over the next four years. The sector could reach $5 billion in revenue by 2024, which is nearly double its 2017 level.

In this market *Cybersecurity Australia* is a vital platform for cybersecurity product and services information and insights into security strategies, emerging cyber threats and leading industry solutions. The resource guide offers the distinct advantage of a specifically targeted interdisciplinary audience of key purchasers and decision makers for your marketing campaign.

Cybersecurity Australia is published twice a year in both print and digital formats to maximise the networking and dissemination of businesses and services in the industry.

In hardcopy, *Cybersecurity Australia* is direct mailed to over 5,000 cyber risk management and security governance associations, retail businesses, critical infrastructure, mining and transport operators, banking institutions, telecommunications, legal, financial and insurance services, information technology businesses, as well as state, territory and federal government organisations in healthcare, social care, education, police and defence.

The *Cybersecurity Australia* digital edition flipbook and mobile responsive micro-site provides an unlimited audience for your business message across social media platforms with direct hyperlinks to your website to seamlessly connect more trade to your business.

The *Cybersecurity Australia* digital edition will also be distributed to approximately 2,500 exhibitors and attendees at the Security Exhibition and Conference held in August at the International Convention Centre, Sydney. This is an ideal network to further share information about your business to those seeking the latest security solutions to avoid cyber threats.

Whether you are eager to optimise your networking or introduce new products or services to the industry, *Cybersecurity Australia* provides you with a highly effective channel that will connect you to a specifically targeted market that is seeking to manage cyber risk and strengthen their defences.

Publisher
ARK Media

Snapshots of the sector

COVID-19 has increased the need for remote working operations and as a consequence, there has been a significant increase in the need to ensure remote working arrangements are secure.

Trends such as Software as a Service (SaaS), cloud storage and cloud computing increase the need to rely on internet connections for basic computer needs.

Australian cybersecurity providers are generating $3 billion in revenue from the domestic market.

Cybersecurity industry revenue has grown at an annualised 10.5 per cent over the last five years and is now worth $1.9 billion in revenue.

Cybersecurity industry revenue is forecast to grow at an annualised 7.8 per cent over the next five years to reach $2.8 billion.

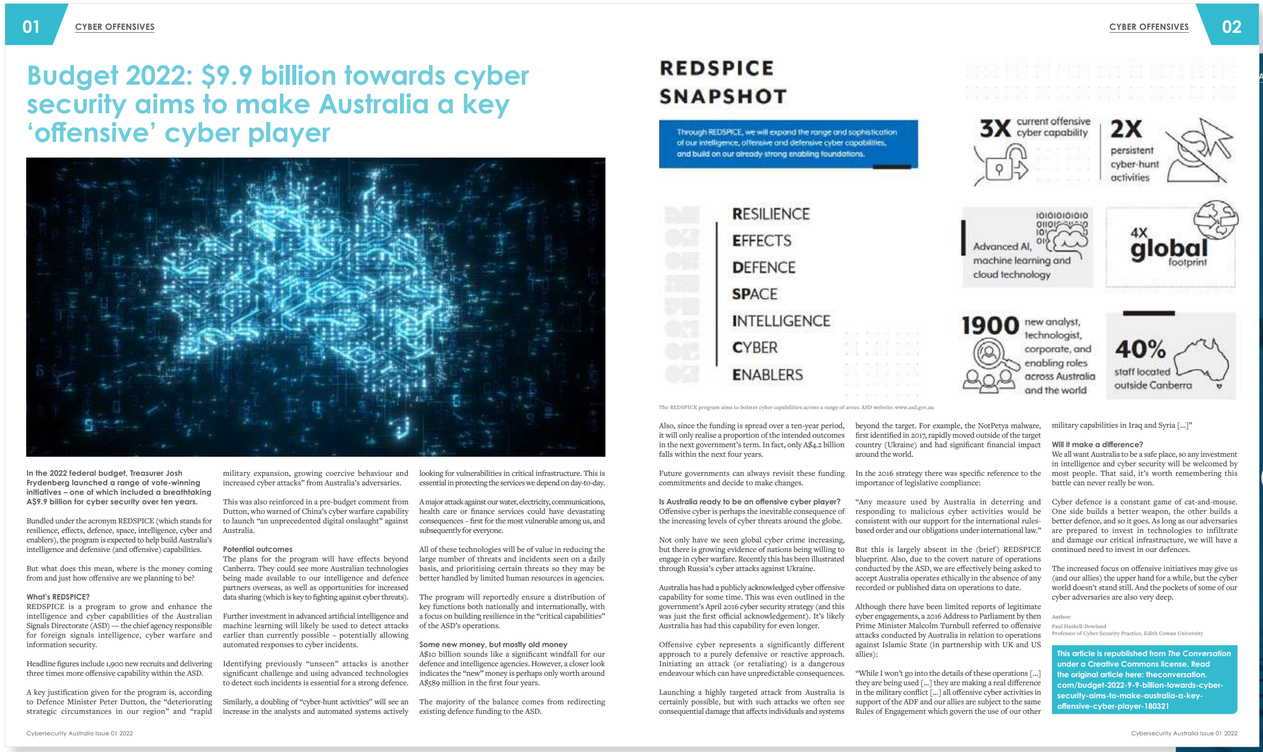
Consumers and businesses rely more heavily on internet based services as systems become increasingly complex. End users will be required to know more about cyber safety to prevent cyber attacks.

Australians spent approximately $5.6 billion on cybersecurity in 2020 - a figure that is expected to increase to $7.6 billion by 2024.

Strong job creation in cybersecurity is likely to continue, with 7,000 more jobs expected to be added to Australia's economy by 2024.

Rates + Sizes

Cybersecurity Australia works for industry businesses in many ways. Its biannual schedule allows businesses to build brand awareness with economical rates. The publication's high quality and format presents business with the best opportunities to showcase their product or expertise through special features and key placements.



01 CYBER OFFENSIVES

Budget 2022: $9.9 billion towards cyber security aims to make Australia a key 'offensive' cyber player

In the 2022 federal budget, Treasurer Josh Frydenberg launched a range of vote-winning initiatives – one of which included a breathtaking A$9.9 billion for cyber security over ten years.

Bundled under the acronym REDSPICE (which stands for resilience, effects, defence, space, intelligence, cyber and enablers), the program is expected to help build Australia's intelligence and defensive (and offensive) capabilities.

But what does this mean, where is the money coming from and just how offensive are we planning to be?

What's REDSPICE?
REDSPICE is a program to grow and enhance the intelligence and cyber capabilities of the Australian Signals Directorate (ASD) — the chief agency responsible for foreign signals intelligence, cyber warfare and information security.

Headline figures include 1,900 new recruits and delivering three times more offensive capability within the ASD.

A key justification given for the program is, according to Defence Minister Peter Dutton, the "deteriorating strategic circumstances in our region" and "rapid military expansion, growing coercive behaviour and increased cyber attacks" from Australia's adversaries.

This was also reinforced in a pre-budget comment from Dutton, who warned of China's cyber warfare capability to launch "an unprecedented digital onslaught" against Australia.

Potential outcomes
The plans for the program will have effects beyond Canberra. They could see more Australian technologies being made available to our intelligence and defence partners overseas, as well as opportunities for increased data sharing (which is key to fighting against cyber threats).

Further investment in advanced artificial intelligence and machine learning will likely be used to detect attacks earlier than currently possible – potentially allowing automated responses to cyber incidents.

Identifying previously "unseen" attacks is another significant challenge and using advanced technologies to detect such incidents is essential for a strong defence.

Similarly, a doubling of "cyber-hunt activities" will see an increase in the analysts and automated systems actively looking for vulnerabilities in critical infrastructure. This is essential in protecting the services we depend on day-to-day.

A major attack against our water, electricity, communications, health care or finance services could have devastating consequences – first for the most vulnerable among us, and subsequently for everyone.

All of these technologies will be of value in reducing the large number of threats and incidents seen on a daily basis, and prioritising certain threats so they may be better handled by limited human resources in agencies.

The program will reportedly ensure a distribution of key functions both nationally and internationally, with a focus on building resilience in the "critical capabilities" of the ASD's operations.

Some new money, but mostly old money
A$10 billion sounds like a significant windfall for our defence and intelligence agencies. However, a closer look indicates the "new" money is perhaps only worth around A$589 million in the first four years.

The majority of the balance comes from redirecting existing defence funding to the ASD.

The REDSPICE program aims to bolster cyber capabilities across a range of areas. ASD website: www.asd.gov.au

CYBER OFFENSIVES 02

Also, since the funding is spread over a ten-year period, it will only realise a proportion of the intended outcomes in the next government's term. In fact, only A$4.2 billion falls within the next four years.

Future governments can always revisit these funding commitments and decide to make changes.

Is Australia ready to be an offensive cyber player?
Offensive cyber is perhaps the inevitable consequence of the increasing levels of cyber threats around the globe.

Not only have we seen global cyber crime increasing, but there is growing evidence of nations being willing to engage in cyber warfare. Recently this has been illustrated through Russia's cyber attacks against Ukraine.

Australia has had a publicly acknowledged cyber offensive capability for some time. This was even outlined in the government's April 2016 cyber security strategy (and this was just the first official acknowledgement). It's likely Australia has had this capability for even longer.

Offensive cyber represents a significantly different approach to a purely defensive or reactive approach. Initiating an attack (or retaliating) is a dangerous endeavour which can have unpredictable consequences.

Launching a highly targeted attack from Australia is certainly possible, but with such attacks we often see consequential damage that affects individuals and systems beyond the target. For example, the NotPetya malware, first identified in 2017, rapidly moved outside of the target country (Ukraine) and had significant financial impact around the world.

In the 2016 strategy there was specific reference to the importance of legislative compliance:

"Any measure used by Australia in deterring and responding to malicious cyber activities would be consistent with our support for the international rules-based order and our obligations under international law."

But this is largely absent in the (brief) REDSPICE blueprint. Also, due to the covert nature of operations conducted by the ASD, we are effectively being asked to accept Australia operates ethically in the absence of any recorded or published data on operations to date.

Although there have been limited reports of legitimate cyber engagements, a 2016 Address to Parliament by then Prime Minister Malcolm Turnbull referred to offensive attacks conducted by Australia in relation to operations against Islamic State (in partnership with UK and US allies):

"While I won't go into the details of these operations [...] they are being used [...] they are making a real difference in the military conflict [...] all offensive cyber activities in support of the ADF and our allies are subject to the same Rules of Engagement which govern the use of our other military capabilities in Iraq and Syria [...]"

Will it make a difference?
We all want Australia to be a safe place, so any investment in intelligence and cyber security will be welcomed by most people. That said, it's worth remembering this battle can never really be won.

Cyber defence is a constant game of cat-and-mouse. One side builds a better weapon, the other builds a better defence, and so it goes. As long as our adversaries are prepared to invest in technologies to infiltrate and damage our critical infrastructure, we will have a continued need to invest in our defences.

The increased focus on offensive initiatives may give us (and our allies) the upper hand for a while, but the cyber world doesn't stand still. And the pockets of some of our cyber adversaries are also very deep.

Author:
Paul Haskell-Dowland
Professor of Cyber Security Practice, Edith Cowan University

AIL SECURITY

Security flaws in Microsoft email software raise questions over Australia's cybersecurity approach

On March 2, 2021, Microsoft published information about four critical vulnerabilities in its widely used Exchange email server software that are being actively exploited. It also released security updates for all versions of Exchange back to 2010.

EMAIL SECURITY 04

Microsoft has told cybersecurity expert Brian Krebs it was notified of the vulnerabilities in "early January". The Australian Cyber Security Centre has also issued a notice on the vulnerabilities.

The situation has been widely reported in the general media as well as specialist cybersecurity sites, but often inaccurately. But the situation also highlights a contradiction in government cybersecurity policy.

When governments find flaws in widely used software, they may not publish the details in order to build up their own offensive cybersecurity capabilities, i.e., the ability to target computers and networks for spying, manipulation and disruption. Operations like this often rely on exploiting vulnerabilities in commercial software — thus leaving their own citizens vulnerable to attack as a consequence.

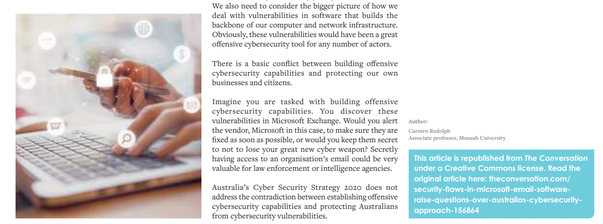
What happened?
Microsoft has issued patches to fix the vulnerabilities and provided advice on how to respond if systems have already been affected.

These vulnerabilities can be really damaging for anybody running their own Exchange mail server. Attackers can run any code on the server and fully compromise a business's email, allowing them to impersonate anybody in the business. They could also read all email stored on the server and potentially compromise more systems within the businesses' network.

Who was affected?
It's important to clear up exactly who the vulnerabilities affected: anybody running their own instance of Exchange, and the risk was higher if web access was turned on.

An ABC/Reuters report said, "All of those affected appear to run Web versions of email client Outlook and host them on their own machines, instead of relying on cloud providers."

But using a cloud-hosted version of Exchange wouldn't necessarily solve the problem, as the vulnerabilities still exist. What's more, larger enterprises will most probably still choose or be required by regulation to also run a local Exchange server that can be exploited in the same way.



Another open issue with moving mail servers to the cloud is that it also gives the provider access to all unencrypted emails by default. End-to-end encryption would increase security, but this is not currently standard practice.

Questions for Microsoft
As vulnerabilities existed in versions of the software released as long ago as 2010, we can assume more skilled attackers have already used them. This raises a fundamental question about the quality of the software, which Microsoft has been developing since 1996. Why did Microsoft not spot these vulnerabilities earlier?

Another question: if Microsoft knew about the vulnerabilities in early January, why did it take two months to alert its customers?

Questions for cybersecurity policy
We also need to consider the bigger picture of how we deal with vulnerabilities in software that builds the backbone of our computer and network infrastructure. Obviously, these vulnerabilities would have been a great offensive cybersecurity tool for any number of actors.

There is a basic conflict between building offensive cybersecurity capabilities and protecting our own businesses and citizens.

Imagine you are tasked with building offensive cybersecurity capabilities. You discover these vulnerabilities in Microsoft Exchange. Would you alert the vendor, Microsoft in this case, to make sure they are fixed as soon as possible, or would you keep them secret to not to lose your great new cyber weapon? Secretly having access to an organisation's email could be very valuable for law enforcement or intelligence agencies.

Australia's Cyber Security Strategy 2020 does not address the contradiction between establishing offensive cybersecurity capabilities and protecting Australians from cybersecurity vulnerabilities.

The establishment of offensive cybersecurity capabilities is explicitly mentioned in the strategy. In contrast, the detection of vulnerabilities with the goal of mitigation is not a clear goal.

Nor is openness about existing vulnerabilities — which would empower Australian citizens to react to them — part of the strategy. Australia has the expertise across the public sector, private sector and civil society to have this important dialogue on how to best protect Australian citizens and businesses.

Author:
Carsten Rudolph
Associate professor, Monash University

Premium Positions*

Outside Back Cover	$5950 + gst
Inside Back Cover	$5500 + gst
Inside Front Cover	$5750 + gst
Facing Contents[2]	$5250 + gst
Facing Foreword	$4950 + gst
Double Page Spread	$7250 + gst
Full Page	$4750 + gst

*Includes equal advertorial and full social digital marketing strategy.

Standard Positions

Full Page	$3750 + gst
Half Page	$1950 + gst
Special Positions	*+15%*

Key Dates

Issue 01 distribution: September 2022

*Multiple bookings attract a 5% Discount per edition

Distribution

Circulation: **7,500+**
Print: **5,000**
Digital & Social Media: **Unlimited**
Events: **2,500+** Expo attendees and exhibitors

Trim Sizes w x h

DPS: 470 x 275mm + 3mm bleed minimum
FP: 235 x 275mm + 3mm bleed minimum
HP: 215 x 122mm | QTR: 102 x 122mm

Type Area w x h

DPS: 450 x 255mm | FP: 215 x 255mm