AustCyber
Australian Cyber Security Growth Network

Western Australia
Innovation Hub

Cybersecurity and small business as critical infrastructure in Australia

GOVERNMENT OF WESTERN AUSTRALIA

NEW INDUSTRIES WA

Cybersecurity and small business as critical infrastructure in Australia

Purchase consumer goods like a Smart TV or fridge as part of a stimulus package and one government dollar invested will create $1.50 in the economy.

Fund infrastructure such as a Marina and it will return you $2.40 for every dollar allocated.

Invest in Cybersecurity for small business safety and the economy will generate $4.70 for every dollar spent.

Key Points

As an increasing number of Australian small businesses are working remotely due to the economic shock of COVID-19. They are faced with an increasing volume and variety of malicious cyber-attack. These **hacking attempts threaten to disrupt their business** in the best case and put them out of business in the worst.

The WA AustCyber Innovation Hub modelled the short-term economic impact of **investing $1 million (AUD) into 5000 small businesses** in Western Australia over a six-month period.

There is no **Cyber Triple Zero** phone number to call when a small business falls victim to a cybercrime.

The creation of a **Cyber Intervention Emergency Response** effort will work to prevent disruption of the critical Australian small to medium enterprise supply chain over a six months period.

AustCyber
Australian Cyber Security Growth Network

Western Australia
Innovation Hub

12%

OF SMALL BUSINESS
EXPERIENCE A CYBER EVENT

Cybersecurity protects Australian business and jobs

The balancing act that economies must deal with when any shock occurs often relies on instant decisions or ones that look to the short to medium term. Political efficacy determines what government will do in the very short term. This ensures that popular and necessary decisions are taken such as cash stimulus, welfare payments and short-term debt forgiveness.

While this is prudent in the very short term, the ability to act counter-cyclically is potentially lost as this stimulus has a strong focus on aggregate demand. The lever of using consumer and business consumption is blunted the longer that stimulus is required in the economy.

The larger, but less popular option, is for significant 'pump-priming'. This form of Keynesian stimulus has a longer tail and fortifies an economy against shock as it navigates its way out of any crisis or economic disruption. At times like this, the private sector is often unwilling to invest. When government sends clear signals of economic leadership, the private sector will add its investment to aid recovery, but not before.

The WA AustCyber Innovation Hub modelled the economic impact of investing $1 million (AUD) into 5000 small businesses in Western Australia over a six-month period. The goal of this investment scenario is to prove that small businesses with a basic understanding and implementation of some or all the Essential 8 Cyber Mitigation Strategies will have better cybersecurity protection and can withstand attacks. In this way, if a small business is ignorant of, or chooses not to deploy basic cybersecurity, it can be argued there is a societal cost where failure to act can cause spill over costs to others.

Poor cybersecurity is a negative externality to society, in the same way as there are spill over costs from traffic congestion and the generation of excessive household waste. Human and physical systems bear the burden of unintended consequences when secondary effects are not considered or ignored. The COVID-19 pandemic has many examples of this.

Cyber savings could buy a Busselton Saw Mill producing furniture for national and international buyers (Walk-in Walk-out) with significant inventory and machinery

Business Risks and Costs of Cyber Attacks to Small Business in Western Australia

7000 $ **COST FOR EACH** CYBER ATTACK

4.7 MILLION $ **SAVINGS FROM** CYBER PROTECTION

150 MILLION $ **COST TO WA ECONOMY** ANNUALLY FROM CYBER ATTACKS

12 % **OF SMALL BUSINESS** EXPERIENCE A CYBER EVENT

Just in the first year cyber savings could buy:

Busselton Saw Mill

producing furniture for national and international buyers (Walk-in Walk-out) with significant inventory and machinery

Software for Horizon Power

to control 'Access and Identity Management' for all staff and contractors for 5 years across WA

62 Rooms 5-Star Freehold Motel

in Halls Creek & Freehold Apartment Complex in Carnarvon

AustCyber
Australian Cyber Security Growth Network

Western Australia Innovation Hub

$7000

COST FOR EACH CYBER ATTACK

If government diverts some of its emergency funds to the large basket of opportunities considered to be 'infrastructure funding', then roads, ports, freight and logistics hubs, rail and next generation utilities projects come to mind. Often in the hundreds of millions and low billions, these projects have a lasting economic multiplier. Positive impacts on an economy are often two and three times the initial investment.

Any large infrastructure project, often in the form of significant built form or capital works spend, needs to be seen through the lens of 'whole of life economic impact'. For example, a greenfield marina development that can be used for commercial fishing, boat lifting, tourism, hospitality, accommodation and commercial services will yield jobs in the phases of infrastructure provisioning, construction and operation. The final demand multipliers confirm that, for every $1 invested now, an average of $2.40 will be generated in terms of local demand and wealth generation. The consumption of white goods and household goods on the other hand like buying a new fridge or Smart TV will yield about $1.50 to a local economy.

The effect of investing in Australian cybersecurity products, services and people during an economic crisis can be quantified in the same way as the two examples above. It takes courage to advocate for 'whole of life economic impact' during a time of spend or perish.

The longer it takes to show the general public the impact of a stimulus decision, the more nervous a government agency becomes in advocating to fund structural projects. The issue here is that, absence a ribbon-cutting ceremony for a road or vital hospital equipment, knowledge economy stimulus seems far less tangible and real.

As an increasing number of Australian small businesses are working remotely, they are faced with a higher volume and variety of malicious cyber-attack. These hacking attempts threaten to disrupt their business in the best case and put them out of business in the worst. The model demonstrates that, for every $1 spent to assist small business with cyber-resilience measures, $4.70 is returned to, and retained by, the Australian economy.

The result is that those small businesses remain open to trade and are not shut down. Businesses and government agencies are now looking at the world through a risk management and mitigation lens. Business continuity is now viewed in terms of survival rather than predicted opportunity. This will change.

Cyber savings could buy a 62 Rooms 5-Star Freehold Motel in Halls Creek & Freehold Apartment Complex in Carnarvon

$4.7m

SAVINGS FROM CYBER PROTECTION

Case Study: Economic Impact, Small Business and Surviving COVID-19

The WA AustCyber Innovation Hub and Edith Cowan University have worked together to increase the basic resilience of micro and small businesses to cyber-attack over the past few years. The Cyber Check Me program has created a small 'cyber-army' of University and TAFE Computer Science Cybersecurity students who work with small businesses to increase their cyber-hygiene practices.

The NSW and Tasmanian AustCyber Innovation Nodes have now agreed to join the effort and participate in a national proof-of-concept and roll out. The South Australian Node is also considering how to work with WA and roll out a pilot as part of a coordinated national effort.

In the pre-COVID world, visits to the Cyber Check Me pop-up stands at business events across WA numbered in the hundreds, with the number of one-on-one consultation registrations at well over 100. The motivations of a cyber-attack do not need to be known. The fact is that a cyber-attack can damage or destroy a business instantly. Every small business just needs to remember it is better to build a fence at the top of a hill than a hospital at the bottom.

> *"We are a well-established building, construction, maintenance and consulting company servicing the Pilbara region for over 20 years. We are increasingly relying on transacting through a variety of digital platforms. We also understand the risk of being put out of business if we are victim to cybercrime. We attended the Cyber Check Me program training in Karratha last year and we are certainly more vigilant these days when it comes to our online and cyber practices. "Sandi and Travers Clarke Trasan Company Founders and Owners*

Cyber Check Me engages with small business through an initial survey benchmarking the practices of each business, a one-on-one consultation (previously face-to-face and now migrating to virtual) and a small report of areas to consider and improve. The program is supported by foundation local government and TAFE members, and is funded mainly by local government authorities who want to assist the small businesses in their area. The local government economic development departments have great access to, and engagement with, their local businesses. These officers are usually the champions for the program.

Cyber savings could buy Software for Horizon Power to control 'Access and Identity Management' for all staff and contractors for 5 years across WA

$150m

COST TO WA ECONOMY
ANNUALLY FROM CYBER ATTACKS

"As a digital company founded on the principles of creating unique intellectual property that will change the way building approvals are reviewed and approved, we are grateful for programs such as Cyber Check Me. It is vital that small businesses remain vigilant when they send sensitive internal or customer documents to one another. Cyber criminals can profit from your naivety or your laziness, and it is too easy to become complacent." Tom Young, Founder and CEO uDrew. WA Innovator of the Year 2018

The economic impact model created by the WA AustCyber Innovation Hub used baseline input data to quantify the opportunity using key input variables to generate a multiplier benefit to the WA economy. Factors such as the percentage of SMEs experiencing cyber-attack, cost per attack, reference data such as insurance reports, impact of cybercrime reports and relevant industry reports were used to better understand the scale of the problem for the WA small business sector.

The model also acknowledges the fact that most small businesses don't even know when they are being attacked (asymptomatic) or have been attacked. They are also unaware of the potential disruption and immediate loss of income this can cause. Many businesses remain unaware until the hack is potentially deep, pervasive in critical business systems or catastrophic.

You can't emerge from a crisis ready to do business when your small businesses don't emerge in the shape you expect them to. Preparedness and disaster recovery planning needs to occur now. A rapid-fire inoculation of Australian Business Numbers (ABNs) would allow the Australian supply chain to not only survive, but to emerge resilient as post-COVID demand increases.

A cyber-army of undergraduate computer science cyber students, coupled with any underutilised WA cybersecurity services companies could be rapidly deployed, and the Essential 8 used as a basic cyber-survival toolkit. Simple tips and techniques include the use of strong passphrases, password protection on home routers and modems, downloading the latest software patches, installing virus and malware updates, data backup techniques and how to encrypt internet connections.

The data captured, stored, and analysed as a result of the small business cyber surveys is also a significant by-product that will give rich insights into the functioning and behaviour of the supply chain when distortions and disruptions occur. Sugar-hit economic stimulus packages while necessary, do not remedy the whole story of business continuity. A repeat of the 'Pink Batts' stimulus leaves us with little insulation from cyber-attacks on Australian businesses.

If government invests in cybersecurity for its critical small business supply chain now, when borders re-open, Australia will be out of the gates long before others are even able to take orders and ship product

Author

DR. IAN MARTINUS
DIRECTOR OF THE WA AUSTCYBER INNOVATION HUB

Trade and investment specialist with experience in technology-related ventures across government and industry. With a strong background in entrepreneurship and innovation, he has founded start-ups in digital visualisation, e-commerce and online music. Cross-border economic empowerment projects for USAID, the World Bank an AusAID include countries such as Iraq, Afghanistan, Pakistan and South Africa. Commercial experience in Japan and with Japanese joint venture companies based in Australia.

As an active member of the economic development communities of Australia and the United States, Ian has delivered successful projects in the urban and land development sectors and co-created the Railsmart project in WA which received an Australian Smart Cities award in 2019. As a founder of two digital start-ups and with Tech Crunch DISRUPT pitch experience, Ian has also worked in California for Fortune 200 tech company SAIC in the Next Generation Networks team, and for the Emerging Markets practice for Deloitte in Washington DC.

His latest role within the Australian cybersecurity ecosystem aims to drive commercial opportunities through alliance projects involving research, business and government partners. He is responsible for promoting all the elements of sovereign cybersecurity capability with a view to partnering appropriately to build export opportunities.

Contributions acknowledgement:
Tony Marceddo – Director for Securing Digital Futures, Edith Cowan University

Darryl Daisley – Director Customs and International Trade, Pitcher Partners WA

This article is Part II in a series of articles under this public/private collaboration between the partners.

WA AustCyber Innovation Hub

WA is a proud member of the Australian Cyber Security Growth Network; a highly coordinated group of the states and territories. The major focus in WA is to create jobs within the emerging cyber security industry.

We assist the creation and protection of Australian companies who create innovative IP.

We align with, and commit, to national priorities as defined by AustCyber's Strategy and Sector Competitiveness Plan.

The WA AustCyber Innovation Hub's focus is on 3 main areas: **critical infrastructure, cyber crime and big data.**

We work across academia, government and industry to increase local jobs.

Our motto of **"partner, build, export"** seeks to create a responsive network of trusted partners who want to grow the industry and Australia's capability in the rapidly changing world of intellectual property and value creation.

We support the innovative initiatives of education providers working with school groups and specialist programs created to inspire the next generation of cyber security start ups.

We encourage partnership with the innovation community in WA, of which AustCyber and the WA AustCyber Innovation Hub are an integral part.

We understand the creation of new IP and new companies takes courage and risk and are willing to support programs, initiatives and ventures that see a path to market in WA and beyond.

We work with partners to ensure the security of their assets, operations and their innovations. We know this type of collaboration will grow local skills and local jobs.

i.martinus@ecu.edu.au | www.wacyberhub.org

Critical Infrastructure | Cyber Crime | Big Data

City of Joondalup

ECU Australia Edith Cowan University

Government of Western Australia

New Industries WA

AustCyber Australian Cyber Security Growth Network

Western Australia Innovation Hub