Deloitte.

Cyber Smart: Enabling APAC businesses

VMware

Deloitte
Access Economics

Executive summary

Digital businesses perform better; they generate more revenue, export more and innovate.

Yet, three in five businesses in the Asia Pacific region have put off digitisation out of fear of cyber attacks.

The COVID-19 pandemic is likely to increase the importance of cyber security. The likelihood and impact of cyber risks is increased with remote and mobile working.

The challenge for both businesses and governments is to make sure they are protected, and prepared.

This report analyses cyber exposure, preparedness and economic opportunity across 12 economies in APAC.

Improving preparedness could increase APAC GDP by $145bn in the long term.

Three in five businesses in APAC are putting off digitisation out of fear of cyber crime. Businesses who are more certain that cyber risks would be effectively managed are more willing to embrace technology. This improves productivity and decreases risk aversion.

It could spur the growth of what is already a $22bn industry.

Cyber crime is listed as one of the top five risks globally. In total, a large organisation in APAC could lose US$30 million in the event of a cyber breach. This is spurring a growing industry, with CAGRs of around 15%.

Are we ready to embrace the opportunity?

Looking at government frameworks and organisational capability across the region, we find that nations with higher exposure tend to be more prepared. But with an average index score of 56 out of a best practice of 100, APAC's preparedness must improve.

Our more developed economies are the most exposed.

This report calculates the exposure of APAC countries to cyber risks. All countries have exposure. It's higher in Singapore, Japan and Australia, and lower in Vietnam, Sri Lanka and Indonesia. This is driven by differing attack surfaces and the potential value of an attack.

Governments can support cyber smarts.

Government can improve cyber frameworks, harmonise regulation, review reporting, and lead from the front with their own processes and procurement. Addressing cyber skill shortages will also be important to minimise risk and harness economic opportunities.

But businesses should adopt best practice.

From two-factor authentication to micro-segmentation, businesses can act today to better prepare for cyber risks, and capture the benefits of digital in the future.

Contents

Invest in cyber to seize digital opportunity

Cyber exposure and preparedness

Spotlight on policy

Invest in cyber to seize digital opportunity

Cyber attacks are one of the biggest risks faced by businesses and governments in the region. Being prepared for attacks by investing in cyber security is not just good sense; it's also an economic opportunity.

Cyber smart: investing with confidence

The economic benefits of digital are well established. Digitally engaged businesses typically perform better than other businesses. They are more likely to be growing in revenue, be exporting, and be innovating.[1]

While businesses in APAC are increasingly digitally engaged, there is significant further potential. Only 60% of businesses in the region had an internet connection in 2016.[2]

There are a number of reasons that businesses may not be digitally connected. One of these is a fear of cyber. Three in five businesses in APAC have put off digital transformation because of this fear. [3] The COVID-19 pandemic is likely to increase the importance of cyber security. The likelihood and impact of cyber risks is increased with remote and mobile working.

Businesses face many risks on a daily basis, from hiring, borrowing and expanding, to theft and fire. These risks do not deter businesses from operating and growing, but rather businesses take steps to mitigate these risks. Similar steps should be taken for cyber risk.

Businesses should embrace the opportunities that digital brings, and ensure that they have appropriately managed the associated cyber risks.

If Australia can capture the cyber opportunity, businesses can invest with confidence. Deloitte Access Economics modelling looked at a scenario where organisations have confidence that cyber risks are well managed.

This scenario was modelled using Deloitte Access Economics' specialised, in-house Horizon model. The Horizon model is capable of forecasting hundreds of economic indicators for multiple regions and industries across different scenarios.

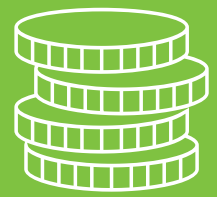
In this scenario, there is a reduction in risk aversion when evaluating new technology and digital projects. This supports a higher adoption rate of new technologies, in turn leading to higher levels of capital investment and productivity growth.

This could lift annual real GDP by 0.7% over ten years. Across 12 APAC countries, this would translate to a lift in GDP of US$145 billion in the long term.

A cyber smart APAC could capture an additional GDP of

US$145bn

over 10 years



The three benefits of investing in cyber security – avoiding the costs of cyber attacks, building a bigger cyber industry, and allowing more businesses to invest with confidence in new digital technologies – represent a significant opportunity.

The growing cyber industry

Historically, businesses have invested in cyber protection measures to mitigate against the potential cost of attacks. This investment has grown significantly enough to become an important digital sub-sector in its own right.

Globally, the cyber security market is expected to reach US$170 billion by 2020.[4]

This is particularly true in APAC, which experiences the highest cyber losses (as a proportion of gross regional product) globally.[5] As a result, governments have invested in dedicated initiatives to capture the cyber opportunity, including AustCyber in Australia and the Cyber Security Agency in Singapore. Cyber spending in APAC is expected to grow faster than the global average with an additional $31 billion spent by 2026.[6]

Businesses in the region are significant buyers of cyber security solutions. Cybersecurity expenditure in Southeast Asia alone was estimated at US$1.9 billion in 2017. This is projected to grow to US$5.5 billion by 2025.[7]

As a result, **the cyber security market in APAC was valued at US$22 billion in 2017.**[8]

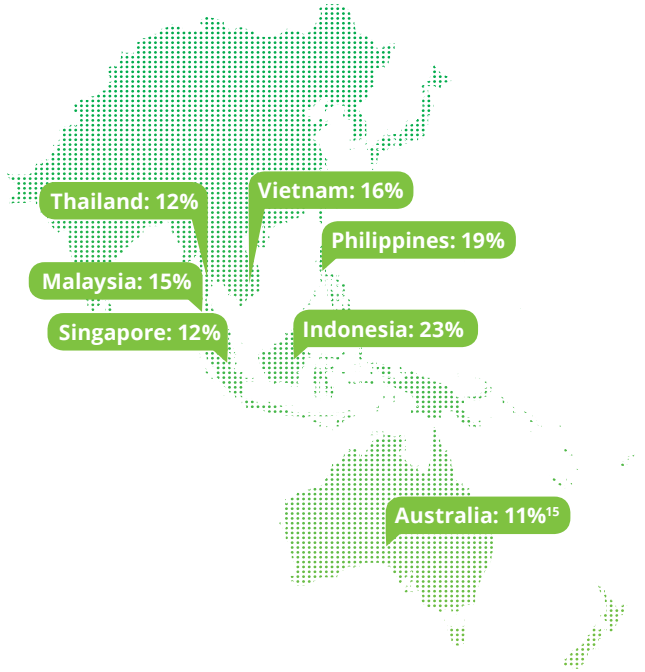
The market is predicted to grow quickly:

- AustCyber expects a CAGR of 15% between 2015 and 2025 (Figure 2)[10]
- Mordor Intelligence predicts a CAGR of 10%, with the industry reaching US$38 billion by 2023[11]
- Gartner data forecasts a CAGR of 15.7% in the Indo-Pacific[12]
- Reuters expects a CAGR of 20%.[13]

As Asia develops its cyber systems, this presents an opportunity for services exports. Countries with leading cyber capabilities may enjoy a competitive advantage, and win cyber business in countries with lagging policy/regulatory environments. There is also likely to be participation of cyber experts from mature markets in the US and Europe. Countries will also need to have investment regulations setting right if they wish to encourage global players to establish locally to deliver bespoke cyber services in-market.

One example effort of trying to build the cyber ecosystem is CyRise in Melbourne, Australia. It is a 'venture accelerator program, powered by Dimension Data / NTT and Deakin University.' It is about leveraging networks to help local businesses take their ideas global.

Figure 2: **National growth in spending on cyber security**[14]



The growing cost of cyber in APAC

The World Economic Forum (WEF) listed cyber attacks as one of the top five global risks for 2019 – topped only by natural phenomena. This is driven by a view that cyber attacks are both likely and high impact.[16]

It is estimated that cybercrime cost US$171 billion in APAC in 2018.[17]

Already, a business somewhere in the world falls victim to a ransomware attack every 14 seconds,[18] and the cost of a typical cyber attack has increased 72% in the last five years.[19]

In APAC, the growing speed and scope of digital transformation, along with the increasing number of targetable devices, are creating a 'perfect storm' for cyber attacks.[20] Almost half (45%) of businesses in APAC have experienced some kind of security attack in the past 12 months, and 63% have experienced business interruption due to a security breach.[21]

As the digital economy continues to grow in the region, so too will exposure to cyber attacks.

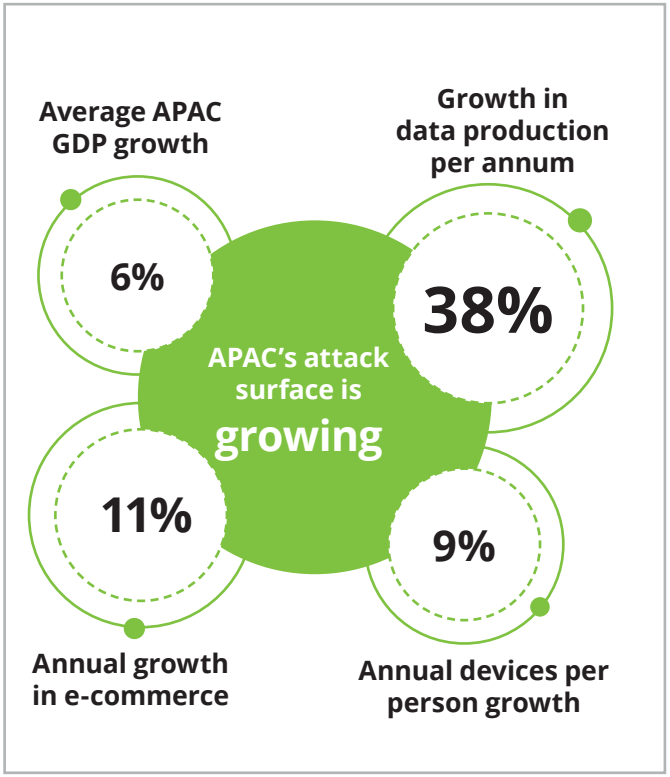
Firstly, more of our day to day devices will be interconnected including our watches, phones, TV's, tablets and home appliances. The number of these devices per person is expected to grow from 2.1 to 3.1 over a five year period.[22]

These devices are creating an increasing amount of data, which also contributes to increased risk exposure. The quantity of data that APAC is producing is growing at 32% per annum.[23]

Secondly, there is more value at risk, as more transactions are online. The value of e-commerce in APAC alone is set to grow at 11% per annum.[24] This rise in online transactions is coupled with a shift towards person-to-person (P2P) and business-to business transactions (B2B). The consequence of this trend is a reduction in transactional security and liability provided by banks and other intermediaries.

The combined result of these three forces – more devices, more data, and more value – creates more incentives for malicious cyber attacks.

With cyber attacks already one of the top five global risks in 2019, this growing exposure requires continued attention from businesses and government.



the cyber **RIPPLE EFFECT**

52%
of businesses in the region engage more than 1,000 third parties in their organisation [25]

83%
of businesses have experienced a third party incident in the last three years [26]

370k
the average additional cost of a data breach if it involves a third-party [27]

The nature of threats is changing

Deloitte's 2019 *Global Industry Threat Assessment* produced a series of industry-focused landscapes to help organisations better understand the types of cyber threat confronting their industry.[28]

It is essential for all organisations to have an up-to-date awareness of the most common threats and tactics, techniques and procedures (TTPs) facing their industry.

Each industry has its own unique set of assets (i.e. sensitive information, specialised infrastructure or services) that make it attractive to cyber-criminals. This also means unique risks.

By understanding the nature of potential threats, organisations are better able to evaluate, manage and ultimately protect themselves against their own unique cyber risks. For example unique industry threats which can have significant consequences include:

- Industrial Control System Threats (ICS) and Wipers in the Energy & Resources industry
- Medical Device Malware in the Life Sciences & Healthcare industry
- Disinformation Campaigns in the Government & Public Services and Technology, Media & Telecommunication industries
- Compromises of Financial Networks in the Financial Services industry.

While businesses face many unique risks, the report also uncovered some threats which are cross-industry and opportunistic. The most common include:

- Ransomware
- Remote Access Trojian
- Information Stealers
- Point-of-Sale Malware
- Distributed Denial-of-Services.

The top four cross-industry TTPs were identified as:

- Spearphishing Attachments
- PowerShell
- Remote Desktop Protocol
- Brute-Force.

Industrial Control Systems Threats in the energy and resources sector[14]

The evolution toward the industrial internet of things has allowed ICS processes in the Energy and Resources sector to become increasingly sophisticated.

Increased interconnectedness of sensors/controllers and enterprise networks is making operations in the sector more efficient. However, legacy ICS systems often lack security controls and often challenging to replace or apply security patches.

If successfully attacked, a breach of legacy ICS systems would have a high impact on any organization. An attack may result in manufacturing disruptions, production downtime, and physical damage to the facility, or even threaten lives.

For example, Deloitte has highlighted a highly-targeted ICS malware dubbed Triton. This malware possesses the capability to modify the logic of the Safety Instrumented Systems controller to disrupt industrial processes monitored by the device.

Recommendations:

- Regularly back up all critical data necessary for business operations.
- Ensure that these file backups are regularly maintained, and stored offline, to prevent the backups themselves from being attacked.
- Deploy & maintain relevant signatures, particularly those related to access attempts.
- Logically separate ICS & Supervisory Control and Data Acquisition implementations & manufacturing networks from the business operating environment.

Why investing in cyber matters for businesses

In total, a large organisation in APAC could lose US$30 million in the event of a cyber breach. For a mid-sized organisation, the cost of a cyber breach could be at least US$96,000.[29] For large companies, like in the Maersk and Equifax attacks, the cost has been considerably higher.

There are a range of business costs associated with a cyber attack. These can be split into:

- direct costs (financial losses such as loss of productivity, fines, and remediation costs)
- indirect costs (opportunity costs such as loss of customers and reputation damage).

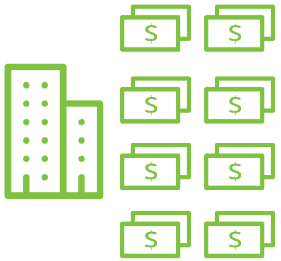
For the average business, Accenture research suggests that the largest costs arising from a cyber attack are information loss (making up 45% of total costs), followed by business disruption (31%), revenue loss (20%) and equipment damages (4%).[30]

The effects of an attack can also be long lasting. Less visible impacts such as loss of intellectual property, or a rise in insurance costs for the business take years to return to normal.[31]

The costs of a cyber attack can also flow beyond the individual business affected. A loss of trust and short-term damage to individual businesses can result in broader economic losses, such as job losses, and declines in customer and enterprise spending.

The threat can also flow through to your broader business network. Research by Carbon Black found that 50% of current attacks use 'island hopping' tactics.[32] These attacks are capable of contaminating a businesses entire supply chain by gaining access to just one point of entry.

With the frequency of attacks continuing to rise, there is a clear rationale for ensuring that businesses are adequately prepared.



US$30 million

for an organisation with more than 500 employees

US$96 thousand

for an organisation with 250 – 500 employees

Cyber smart index: how prepared are we?

The risk of cyber attacks is inevitable. Yet the level of exposure varies. A higher level of exposure to risk requires a higher level of preparedness. Which countries are most exposed?

Measuring our cyber smarts

In our digital economy, cyber risk is inevitable. As the digital economy grows in each country in the region, so too does their exposure to cyber attacks.

Being appropriately prepared is key to meeting these risks, and minimising the potential costs of attack.

In this paper, we construct an index which allows us to compare risk exposure and preparedness across the region.

Constructing the Index.

This report compiles a new index which seeks to capture both the level of cyber risk exposure faced by countries in the region, and the degree of cyber preparedness.

We compile a range of measures across a range of countries, with the goal of helping policy makers and businesses to identify how well placed they are to face the risks in their jurisdiction/s.

In the exposure index, there are two pillars and seven sub-pillars, consisting of 20 unique measures. In the preparedness index there are two pillars and seven sub-pillars, consisting of 23 unique measures.

More details on how the index was constructed are available in the Technical appendix.

To measure risk exposure, the index considers a country's attack surface (the number of potential attack points) and potential attack value (the financial opportunity to attackers). A country's exposure is measured as a proportion of the highest exposure country in APAC, meaning the maximum score is 100.

A country's preparedness score is determined by the sophistication of the legislative environment, and organisational capability to prevent and respond to cyber threats. A country's preparedness score is based on the extent of best practices which are implemented within the country.

How is it different from other indexes?

The Cyber Smart index explored in this report captures the inherent exposure of different economies and preparedness, from both an organisational and legislative perspective.

It also shines a spotlight on APAC specifically.

Other cyber indices.

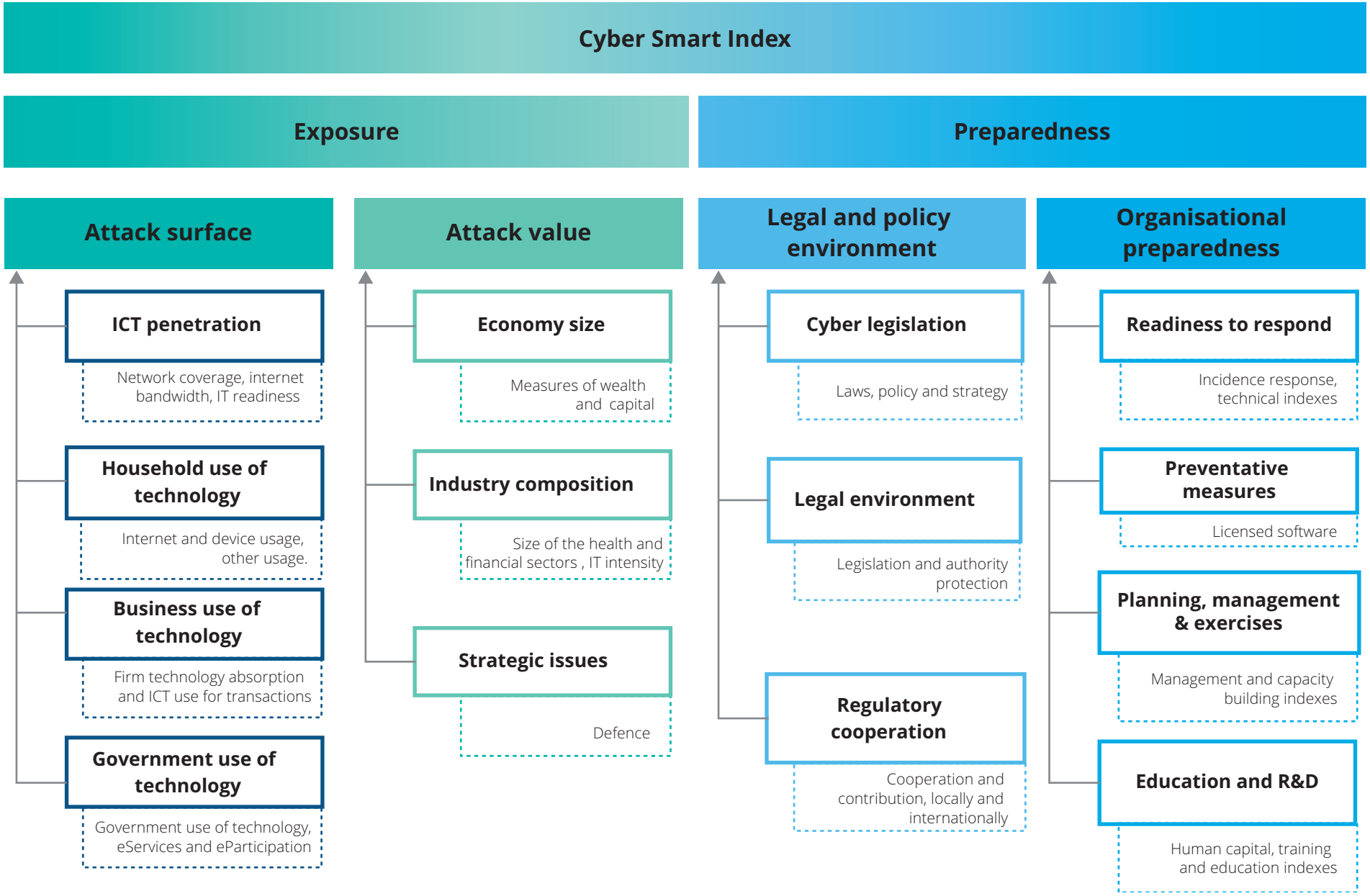
This is not the first index to measure regional cyber security and awareness.

- The *Global Cybersecurity Index (CGI)* measures a country's security by focusing on policy measures, both organisational and legal.
- The *National Cyber Security index* measures security capacities implemented by governments and incident response.
- The *Comparitech* index scored cyber security primarily on the frequency or prevalence of attacks.

The Cyber Smart index

Although other indices play a role in better understanding the cyber landscape, none, to our knowledge, focus on the inherent exposure to cyber attacks. Our approach fills this gap by taking a unique look at the size of the attack surface and the value that's at risk.

Furthermore, within the preparedness measure, the Cyber Smart index considers the actions of business as well as government. Beyond legislative sophistication, this index explores what businesses can do to be better prepared for the growing risk of cyber attack.


Cyber Smart Index
Exposure
Preparedness
Attack surface
ICT penetration
Network coverage, internet bandwidth, IT readiness
Household use of technology
Internet and device usage, other usage.
Business use of technology
Firm technology absorption and ICT use for transactions
Government use of technology
Government use of technology, eServices and eParticipation
Attack value
Economy size
Measures of wealth and capital
Industry composition
Size of the health and financial sectors , IT intensity
Strategic issues
Defence
Legal and policy environment
Cyber legislation
Laws, policy and strategy
Legal environment
Legislation and authority protection
Regulatory cooperation
Cooperation and contribution, locally and internationally
Organisational preparedness
Readiness to respond
Incidence response, technical indexes
Preventative measures
Licensed software
Planning, management & exercises
Management and capacity building indexes
Education and R&D
Human capital, training and education indexes

Cyber Smart Index

The figure on the right shows where each economy sits on the exposure and preparedness indexes. There is generally a positive relationship between exposure and preparedness, however some economies stand out as particularly well prepared, or under prepared, compared to their peers.

Country	Exposure rank	Preparedness rank
Singapore	1	1
South Korea	2	6
Japan	3	2
Australia	4	3
New Zealand	5	5
India	6	7
Malaysia	7	4
Philippines	8	9
Thailand	9	8
Sri Lanka	10	10
Vietnam	11	11
Indonesia	12	12

At a glance

Vietnam ranks 11th on exposure and preparedness, and experiences the highest frequency of cyber attacks. Vietnam does not have comprehensive legislation to deal with data security and privacy.

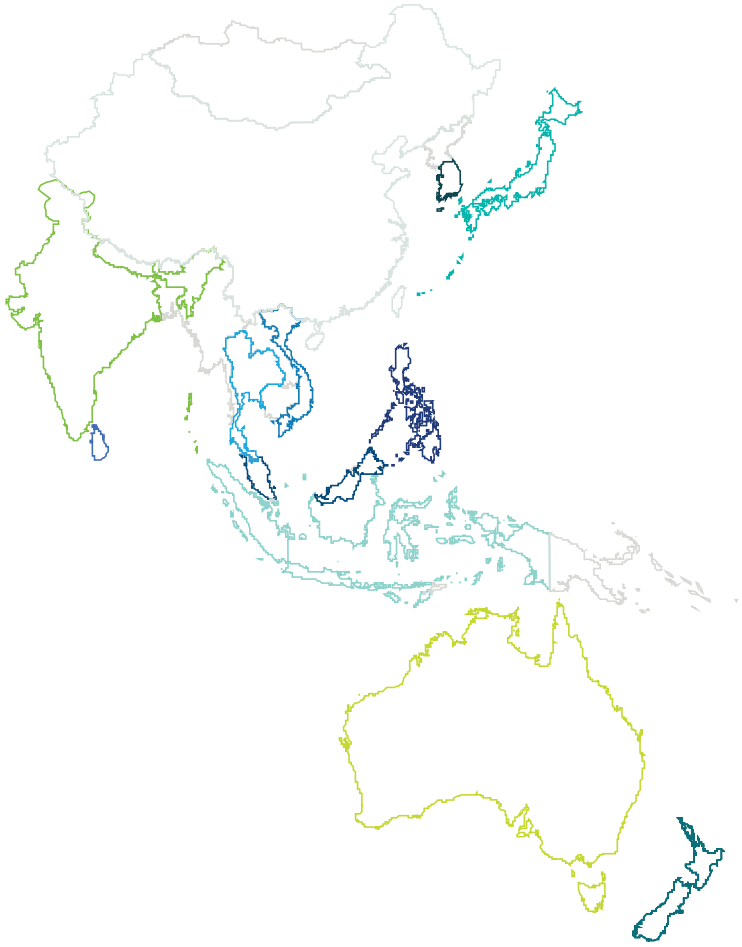
Thailand ranks 8th in preparedness and 9th in exposure, however has one of the highest cyber attack rates in APAC. Growing use of online devices and interest in cryptocurrencies is worsening Thailand's exposure to risks.[1]

Singapore is the most prepared and the most exposed country in APAC. Singapore has a highest rate of ICT penetration due to its small size and strong infrastructure, and also has the highest GDP per capita. Singapore scores consistently high across all measures of preparedness, with sound legal and organisational awareness.

South Korea performs relatively well in preparedness, with high rates of R&D and response time for cyber threats. However, South Korea's high use of technology by business and government, as well as its strategic value, means exposure is also substantial.

New Zealand ranks 5th on both exposure and preparedness. Its recent cybersecurity strategy is expected to improve preparedness, with a focus on being proactive, resilient and responsive.

India ranked 7th on the preparedness index and 6th on the exposure index. There is significant variation in preparedness across the Indian economy.



Malaysia ranks 7th on the exposure index, but 4th on the preparedness index. Strong regulatory cooperation, and a comprehensive privacy regime mean despite less impressive relative organisational capability, Malaysia is ahead of its peers with a similar level of exposure.

The Philippines ranked 9th on preparedness and 8th on the exposure index. It presents a low exposure level with the third lowest GDP per capita, relatively small health and financial sectors and low household internet usage.

Indonesia ranks lower than its ASEAN counterparts despite its large economy and increasing digitisation, largely because of its small services sector. Its exposure is likely to grow in coming years with high rates of growth.

Australia ranked as the 3rd most prepared, and 4th most exposed to risk in the region. Australia particularly has strong cyber legislation, education and R&D.

Japan has the 3rd highest exposure to cyber risk and 2nd highest preparedness in APAC. However, anecdotal industry perspective is that organisational preparedness could be improved.

Sri Lanka has both low exposure and preparedness. Sri Lanka's exposure profile is low given its small economy size and relatively small health and financial sectors, which are sectors that attract cyber attacks.

Country insight

Australia ranked as the third most prepared, and fourth most exposed in the region.

Australia's exposure stems from its large attack surface and value. For example, Australia has the highest proportion of individuals with internet access in the region at 93%, as well as the second largest health sector and third largest financial sector.

Australia is relatively well prepared for cyber, scoring particularly highly in cyber security education and R&D investment, due in part to a strong emphasis in the higher education sector. Universities are a significant contributor to cyber development, spearheading and funding organisations such as AusCERT which has become Australia's primary response unit for cyber attacks.[2]

On the flip side, Australia has some of the most profitable education providers in the world.[3] This is contributing to a cyber threat; the rapid digitisation of Australian education systems and the rise in eLearning has made the edu.au domain the most frequently targeted education domain in the world.[4]

Australia is increasing its cyber capability. According to AustCyber, the value of the Australian cyber security sector is expected to triple by 2026 to AUD$6 billion in annual revenues, creating an additional 18,000 jobs.[5]

Case Study: VMware facilitates the Australian Taxation Office's cloud program[8]

The Australian Taxation Office (ATO) has signed a AUD$17 million, three-year software licensing and support deal with VMware. The deal is set to renew and consolidate multiple separate, existing arrangements held by the ATO, with VMware supporting the security of Australians' personal taxation information. It is expected this deal will improve cost-effectiveness for the ATO as it becomes increasingly technology and mobile-based. Improving cloud capabilities is likely to help the government agency to meet the strategic priorities of the Australian Digital Transformation Strategy, which includes having a government that is easy to deal with, fit for the digital age and informed by citizens.

This is fuelling demand for cyber skills. In 2019, a survey of Australian businesses found 61% find it 'difficult' or 'very difficult' to recruit qualified cyber experts.[6] As a result, the Australian Government has established has established the Academic Centres of Cyber Security Excellence (ACCSE), which aims to address this shortage.[7]

Country insight

Singapore scored the highest in both the preparedness index and exposure index.

Partially due to its small size and centralisation, Singapore has been able to develop a strong mobile broadband network. Singapore boasts the fastest 4G download speed in the world facilitating some of the highest per capita data consumption in the world. Based on the level of internet traffic alone, Singapore is likely to attract cyber attacks.

Aware of the risks posed in the cyber space, Singapore has established a strong legislative environment led by the Cyber Security Agency (CSA). The CSA is responsible for a nation-wide masterplan that aims to create a cohesive effort between business and government to combat cyber threats.[9]

Part of this collaborative effort is the Co-innovation and Development Proof of Concept (POC) scheme, organised by the CSA.[10] This scheme, launched in 2018, provides seed funding and support to promising developments in the cyber security space. In 2018, the CSA reviewed 72 proposals, 8 of which were successful.

Recognising the value as a regional financial hub, the Monetary Authority of Singapore has launched a $30 million cyber security capabilities grant in an effort to support firms in the financial sector to develop their security measures.[11]

Case Study: VMware helps Singapore Airlines to improve their employee experience[12]

VMware is supporting the cyber-secure delivery of Workspace ONE, a mobile application for Singapore Airlines employees. It is anticipated that the app will create a connected and seamless experience for employees, across both personal and company-issued devices, which will enable greater workforce efficiency, mobility and collaboration. VMware will support the company to take advantage of these benefits by improving operational efficiency and data security in the deployment of the app.

How can we boost preparedness?

Exposure to cyber risk is inevitable and will continue to grow with the digital economy.

The index has shown that some countries are better prepared than others for dealing with their given level of cyber risk exposure.

Everyone has a role to play in being prepared for cyber risks. Individuals should be aware of the risks and businesses should go beyond what is required in protecting their data.

The next chapter discusses how government can help society to understand, protect against and respond to cyber threats.

Spotlight on policy

A range of tools available to government

While government can set rules and demonstrates leadership, ultimately the vast majority of factors determining cyber risk and preparedness relate to business and individual activities.

Governments have a range of tools available to manage cyber. These include:

- leading by example, by demonstrating strong understanding of and adherence to cyber security best practice principles inside government departments
- using policy and regulation to set minimum standards for cyber preparedness inside business, as well as policing and penalising cyber criminals
- providing tools, training, resources and other support to businesses to ensure that they are well equipped to prepare themselves for cyber risks.

The challenge for government is to provide a legislative framework and policy environment which allows businesses to innovate, maximising the potential of digital whilst managing the associated cyber risks.

This section provides an overview of some areas where governments of focusing their cyber efforts with specific examples, including:

- leading by example
- regulatory harmonisation
- procurement
- reporting.

This section concludes with a discussion of the need to address cyber skill shortages and a framework and actions for businesses to ensure they are better prepared for the cyber future.

Chart 1: **Percentage of time cybersecurity executives at large companies spend addressing cyber domains**[1]

Leading by example

Governments at both state and federal levels have a significant digital presence. They also hold a wealth of valuable data about individuals, businesses and national matters. In this context, it is crucial that governments themselves observe cyber security best practice.

According to IDC, state/local government bodies are expected to grow their spending on cyber security at a compound annual growth rate of 23.7%. This makes state/local government bodies the fastest growing spenders on security in the region.[2]

This spending is crucial to ensuring that services remain operational and citizen data remains secure. Yet with digital services increasingly critical for governments around the region, spending in and of itself may not be sufficient.

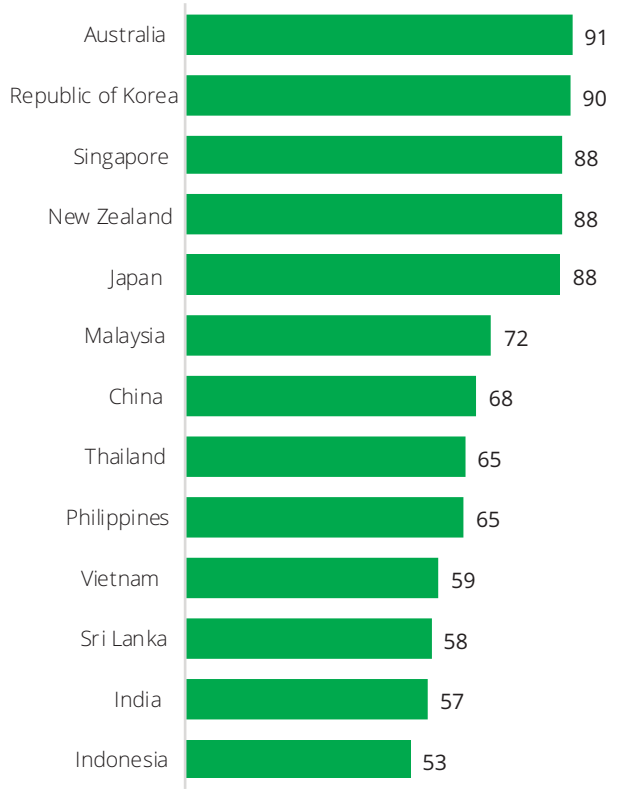
Governments should consider broader governance structures to support any cyber strategy. Specifically, strategy frameworks should consider:[3]

- Strategy and operating model i.e. transformation, assessment, risk management, compliance, training, education and awareness.
- Policies, standards and architecture for security i.e. infrastructure and application protection, vulnerability and access management, information privacy and protection.
- Risk culture and behaviour i.e. advanced threat readiness and preparation, cyber risk analytics, security operations centres and threat intelligence.
- Risk management and reporting i.e. cyber incident response teams and war-gaming.

Recent breaches of government data have illustrated the potential cost of getting it wrong. In July 2018 SingHealth, Singapore's largest healthcare group, was compromised. This was considered to be one of the largest data breaches in the nation's history, with personal data from 1.5 million customers being compromised.

A principles based approach is often a the most effective approach to defining cyber security regulation. For example, Japan's practices a holistic approach requiring cyber-related business to cooperate with government in enhancing cyber security. Legislation also has a focus on developing cyber talent and skills training.[3]

Chart 2: **The e-Gov Index measures the extent in which countries use ICT in public administration**[1]



Regulatory harmonisation

Regulatory approaches to cyber in APAC are varied and localised, as economies with different levels of risk and preparedness approach the issue differently. However, there are potential benefits from harmonising regulations where possible.

As identified in the index, risk levels do vary between countries. Governments take localised approaches to managing cyber risk due to differing levels of risk, policy priorities and capabilities. This is particularly true in APAC, which is economically and culturally diverse.[5]

While local approaches are well justified, they can have flow-on effects. For businesses operating across borders, the need to understand and comply with varying regulations regionally can add regulatory burden without necessarily contributing to stronger preparedness.[5]

For regulators themselves, fragmentation can make it more challenging to penalise cyber crime. Because cyber criminals are not limited by traditional borders, threats can come from anywhere in the globe.[6]

Cyber crime is traditionally difficult to investigate and prosecute. Being able to cooperate internationally is an important component of being able to ultimately enforce local laws.[6]

Harmonisation is not only about aligning regulation between nations. It should also have a focus towards harmonising regulations between sectors in order facilitate proactive cyber security strategies.

The region has already started to harmonise regulation in key areas. For example, APAC Economic Corporation's Privacy Framework introduced a common set of principles to encourage the harmonisation of privacy and data protection rules across the region.[7]

In Japan, regulators have focused on maintaining cross-border data flows, with strong cross-sectoral domestic privacy laws that are regularly re-aligned to take into consideration new technological developments.[5]

The World Economic Forum and Deloitte's latest report discusses five privacy enhancing techniques that allow institutions, customers, and regulators to analyse and share insights from data without distributing the underlying data itself.[8]

These techniques are:

- **Differential privacy:** noise is added to an analytical systems so that it is impossible to reverse engineer the individual inputs.
- **Federated analysis:** parties share the insights from their analysis without sharing the data itself.
- **Homomorphic encryption:** data is encrypted before it is shared, such that it can still be analysed but not decoded into the original information.
- **Zero-knowledge proofs:** users can prove their knowledge of a value without revealing the value itself.
- **Secure multiparty computation:** analysis is spread across multiple parties such that not individual party can see the complete set of inputs.

Procurement

Government in itself is a large buyer of digital services. In implementing cyber security requirements into the procurement process, governments have an opportunity to play a more active role in defining best practice.

As the technical innovation continues to grow throughout APAC there is a increasing need to raise the level of cyber security capabilities in the public service.

Government and regulatory bodies in the region are becoming increasingly cognisant of the need to balance their sustained technical innovation with cyber security protections.[9]

One method of increasing the capabilities throughout the public service is to implement cyber security criteria in the procurement process.[10]

By implementing minimum cyber security criteria there is an opportunity identify potential flaws or conceivable impacts during the sourcing phase.

This can contribute towards reducing the overall costs of responding to a cyber attack and often remediation can be minimised or avoided entirely.

Government procurement practices often have an influence on the broader private sector. For example, approximately 8% of all businesses in Australia are engaged in some form of government procurement.[12]

Taking a proactive stance towards defining best practice in procurement can have an overall impact on broader network security.[10]

Furthermore, such actions could help transition government's image as a body not only being responsible for imposing regulations, to one of a responsible actor defining overall network security.

In defining its procurement criteria, government needs to be careful to not exclude or hamper innovation in smaller firms by imposing over burdensome criteria.

Procurement guidelines

A good example of the implementing cyber security criteria to the procurement process is the Australian Government's procurement guidelines.

The guidelines require that government entities consider and manage their procurement security risk with respect to the Australian Government's Protective Security Policy Framework.[11]

The aim of these guidelines is to reduce the risks, and subsequent costs, associated with procuring services from an external entity.

Reporting

Reporting requirements have an impact on business ability to respond to and track the frequency of cyber attacks. It is important to strike a delicate balance between ensuring trust while not imposing over burdensome requirements.

A nation's regulatory approach to defining and reporting cybercrime and threats will influence the business sector's ability to coordinate with government and regulators to respond to, and record the frequency of, cybercrime.

Regional variation in the reporting standards regarding cyber security threats, such as reporting attempts verses breaches etc., could increase the regulatory burden on businesses operating in the region.

It can be difficult for the business sector to monitor and report all threats, especially considering if the nature of the information is confidential. Over-reporting could potentially lead to a reduced response by business entities when a real risk of harms appears.[13]

However, as the business sector continues to collect and manage personal consumer data, the consequences of poor management becomes increasingly severe.

In essence, reporting regulation must ensure business entities are operating under the best standard of data protection, without imposing unnecessary restrictions on their operations. In Australia, mandatory data breach notification laws were passed in 2017, which require organisations to notify individuals that if a suspected or actual breach of personal information is likely to result in serious harm. The Government conducts and publishes pro-active assessments of organisations.[14]

Data Sovereignty

A data sovereignty approach to cyber security traditionally encompasses some approach towards either national sovereignty, national security or consumer protection.

Data sovereignty exists to some degree in almost every nation throughout the globe. However, the overall aim of the regulatory strategy often differs from country to country.

For example, Thailand's Cybersecurity Act, published on 27 May 2019, is intended to be holistic piece of cyber security legislation aimed at maintaining "national security, economic security, military security and public order" in Thailand.[13]

Regulation in Indonesia, on the other hand, emphasises personal data protection. Under the legislation financial data cannot be stored outside the country without prior approval.[15]

Developing skills

Governments, businesses and educational institutions need to implement and maintain specialised cyber security training to address the skills shortage.

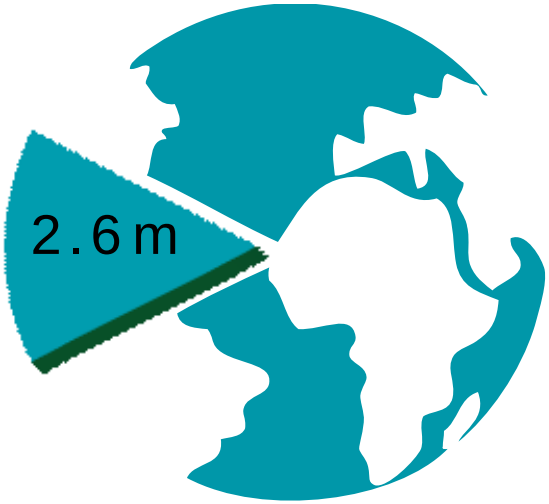
As cyber defences develop, so too does the nature of cyber attacks. Countries need to develop the skills to ensure that businesses are prepared for this threat in the future.

The current skills shortage for APAC is 2.6 million and rising.[17] This represents the largest regional shortage in the world, with the second largest shortage found in Latin America with 600,000 fewer workers than required. This shortage presents a substantial task and opportunity for countries within APAC.

Despite a strong and profitable cyber industry in Australia, 61% of firms stated that employing a qualified cyber professional was 'difficult' or 'very difficult'.[18] Acknowledging the shortage of workers, the Australian Industry and Skills Committee is working towards a national cyber literacy level. This initiative may implement cyber security units in all vocational education and training in Australia, regardless of area of study.[19]

In 2014, Singapore announced its Smart Nation initiative, which intends to bring Singapore to the forefront of digital technology across its economy. Part of this is the Smart Nation Scholarship, which targets high performing students in engineering and IT to help develop the systems to protect Singapore's critical infrastructure.[20] This program seeks to ensure that Singapore's top talent is influencing the direction of the national cyber strategy.

The skills shortage in APAC is



Source: ISC, 2019

A framework for assessing approaches to cyber risk

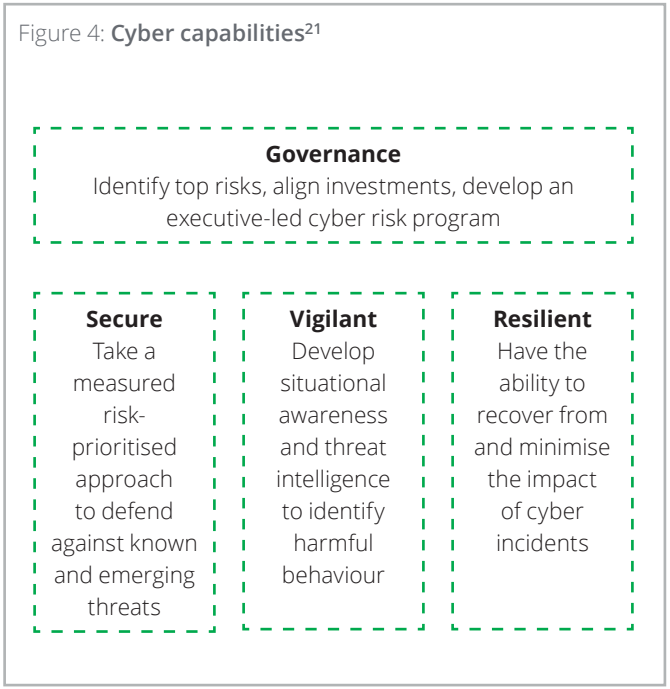
Organisations need a holistic, business-driven and threat-based approach to manage cyber risks. While securing assets is important, being vigilant and resilient in the face of cyber attacks is imperative.[21]

Deloitte's secure, vigilant and resilient approach, which is enabled by effective strategy and governance,[22] is key to managing cyber security risk continued business performance and meeting regulatory expectations.[21]

- An effective cyber **strategy** balances an organisation's strategic objectives and risk appetite by establishing an actionable road-map to support the evolution of security program priorities.
- It is essential to remain **vigilant** towards internal and extranet threats in order to secure against successful cyber attacks.
- However, it is not a question of whether an attack will or will not occur but when. **Resilience** is vital when responding to data breaches and developing business recovery plans.

Effective **governance** is the foundation and starting point for any effective cyber risk management strategy. Ensuring the necessary structures and rules are in place to maintain and enhance preventative and detective cyber security capabilities.[22]

Figure 4: **Cyber capabilities**[21]



A view from VMware

According to VMware, there are five core strategies that are key in moving towards an effective cyber security strategy:[23]

Least Privilege	Users and system components to be allowed only the minimum access and necessary function needed to perform their purpose.
Micro-segmentation	The whole IT environment is divided into small parts to contain the damage if one part of the network is compromised.
Encryption	For critical business processes, all data should be encrypted, while stored or transmitted. So that any breach will result in only obtaining unreadable data.
Multi-factor Authentication	The identity of users and system components should be verified using multiple factors (not just simple passwords).
Patching	Systems should be kept up to date and consistently maintained.

Micro-segmentation

Businesses do not have to wait for government and regulators in order to make themselves cyber smart.

Micro-segmentation is a network security technique that divides a data centre into individual segments (down to the individual workload) and uniquely defined security controls.[24]

Traditional approaches to cyber security tend to focus on preventing a breach by protecting the data centre's perimeter.

The primary issue with this approach is that one portion of the network is breached, there are few controls to prevent threats from moving laterally throughout the network.[25]

Once inside the data centre, an attacker can exploit vulnerabilities inside the data centre to move throughout the data centre with relative ease.

By adopting a segmented approach to network security, with unique controls defined for each segment, cyber threats are essentially isolated form each other inside the network.[25]

Micro-segmentation also allows for increased flexibility in defining security policies, as it removes the need to install multiple physical firewalls. Instead, unique security policies are applied to each individual segment.

Technical appendix

Preparedness and Exposure Index formation

Cyber smart: investing with confidence – modelling GDP

Australia gets cyber smart – Horizon modelling of digital investment

As discussed in Chapter 1, 3 out of 5 businesses in APAC choose not to digitise out of concerns that this would make their business more vulnerable. This reluctance acts as a handbrake on productivity, innovation and growth.

Deloitte Access Economics have previously modelled a scenario where this anxiety is removed and individuals, businesses and governments increase their level of digitisation in Australia.

Using the specialised, in-house Horizon model, Deloitte Access Economics estimated the benefit of a more proactive position on cyber security. This analysis predicted that greater digitisation and cyber awareness led to increased levels of capital investment and higher levels of productivity, which ultimately led to an increase growth by 0.7% over 10 years.

Although this analysis was conducted for Australia only, it is reasonable to except the same relationship to exist between digitisation, productivity and growth for other countries in APAC. Therefore, applying the same improvement to the combined GDP of the countries explored in this analysis, yields an expected impact of at least US$145 billion over the next 10 years.

If anything, this number is likely to be a conservative estimate for APAC. As discussed in this report, Australia has an above average level of digitisation and it is reasonable to expect that the overall APAC region could benefit more broadly from digitisation than in the Australian scenario.

Nonetheless, this number provides a helpful indication of the potential loss generated by reluctance to embrace new technology.

For further details, see What's over the horizon? Recognising opportunity in uncertainty at https://www2.deloitte.com/au/en/pages/building-lucky-country/articles/whats-over-horizon.html.

Deloitte Access Economics' Cyber Smart Index Methodology

Deloitte's Cyber Exposure and Preparedness Indexes have been created by Deloitte Access Economics.

In the exposure index, there are two pillars and seven sub-pillars, consisting of 20 unique measures. In the preparedness index there are two pillars and seven sub-pillars, consisting of 23 unique measures.

We have drawn on the subjective judgement and experience of cyber experts at Deloitte to create this index. We recognise this index isn't precise nor perfect, but it is designed to help citizens, businesses and government understand the relative preparedness independently of cyber risk exposure across APAC.

Country	Exposure Index	Preparedness Index
Singapore	75	84
South Korea	73	63
Japan	72	74
Australia	68	73
New Zealand	61	65
India	57	50
Malaysia	56	72
Philippines	51	45
Thailand	50	48
Sri Lanka	50	39
Vietnam	50	37
Indonesia	46	32

Understanding the index

The average exposure index score is 60.
South Korea has the median number of internet users among the countries in the index. If South Korea were to have the highest number of internet users South Korea's exposure index would increase from 73 to 74.

The average preparedness index score is 56.
Sri Lanka has the median score for the human capital index, within the organisational preparedness pillar. If Sri Lanka were to have the highest human capital index score (currently held by Australia), Sri Lanka's their preparedness index would increase from 39 to 40.

The **Philippines** has the median score for the cyber policy and strategy indicator. If the Philippines were to have the highest score for this indicator (currently held by Singapore), their preparedness index would increase from 45 to 47.5.

Exposure Index: The attack surface pillar contains four equally weighted sub-pillars

'ICT penetration' relates to the extent that using the internet is accessible. It contains three equally weighted measures:

- Mobile network coverage as a percentage of population (Source: World Economic Forum Networked Readiness Index)
- International internet bandwidth, kb/s per user (Source: World Economic Forum Networked Readiness Index)
- IT readiness and broadband deployment (Source: BSA The Software Alliance and Galexia Cloud Computing Scorecard)

'Household use of technology' contains two equally weighted indicators"

'Internet and device usage' is based on four equally weighted measures:

- Total internet users (Source: World Economic Forum Networked Readiness Index, population data from World Bank)
- Households with internet access as a proportion of all households (Source: World Economic Forum Networked Readiness Index)
- Internet Access in Schools as a proportion of all schools (Source: World Economic Forum Networked Readiness Index)
- Total mobile subscriptions (Source: World Economic Forum Networked Readiness Index, population data from World Bank)

'Other household use' is based on two equally weighted measures:

- B2C Internet use (Source: World Economic Forum Networked Readiness Index)
- Number of e-commerce users as proportion of population (Source: e shop World)

'Business use of technology' contains two equally weighted measures:

- Firm level technology absorption (Source: World Economic Forum Networked Readiness Index)
- ICT use for B2B transactions (Source: World Economic Forum Networked Readiness Index) '

'Government use of technology' contains three equally weighted measures

- ICT use and government efficiency (Source: World Economic Forum Networked Readiness Index)
- Online Service Index (Source: UN E-government Index)
- E-participation Index (Source: UN E-government Index)

Exposure Index: The attack value pillar contains two equally weighted sub-pillars

'Economy size' relates to general value available in the economy. It contains four equally weighted measures:

- GDP per capita (Source: World Bank)
- GDP (Source: World Bank)
- Services as a proportion of total GDP (Source: World Bank)
- Capital Index (Source: IMD World Digital Competitiveness Ranking 2019, IMD)

'Industry composition' relates to industry specific and capital risks. It contains three equally weighted measures:

- 'Health sector as a proportion of total GDP (Source: World Bank)
- Domestic credit as a proportion of total GDP (proxy for financial sector) (Source: World Bank)
- Resident patent applications per million people (Source: World Intellectual Property Indicators (WIPO))

Strategic risk measures a country's geopolitical risk that may affect their attack value. It contains one measure:

- Militarisation score (Source: Global Peace Index, VisionOfHumanity.org)

Preparedness Index: The legal and policy environment pillar contains three equally weighted sub-pillars

'Cyber legislation' relates to government's administration over cyber-related issues. It contains two equally weighted indicators:

'Cyber laws' is based on two equally weighted measures:

- Global Cyber Legal Index (Source: ITU; calculated using 2018 Global Cyber Index value and 2015 proportion of legal pillar)
- A score out of six of a series of questions regarding cyber laws and regulations (Source: BSA The Software Alliance and Galexia Cloud Computing Scorecard)
  - Is there a personal data breach notification law or regulation?
  - Is an independent private right of action available for breaches of data privacy?
  - Is there a national cybersecurity strategy in place?
  - Is the national cybersecurity strategy current, comprehensive, and inclusive?
  - Are cybercrime laws or regulations in place?
  - Are cybercrime laws or regulations consistent with the Budapest Convention on Cybercrime?

'Cyber policy and strategy' is based on two equally weighted measures:

- Global Cyber Organisational Index (Source: ITU; calculated using 2018 Global Cyber Index value and 2015 proportion of organisational pillar)
- Cyber security policy index (Source: National Cyber Security Index)

'Legal environment' relates to general government and regulatory administration over ICT-related issues. It contains two equally weighted indicators:

''Legislation' is based on two equally weighted measures:

- Laws relating to ICTs (Source: World Economic Forum Networked Readiness Index
- A score out of 14 of a series of questions regarding general data privacy, security and intellectual property laws and regulations (Source: BSA The Software Alliance and Galexia Cloud Computing Scorecard)
  - Is a data protection law or regulation in place?
  - Is a data protection authority in place?
  - Are data controllers free from registration requirements?
  - Are there laws or appropriate guidance containing general security requirements for cloud service providers?
  - Are laws or guidance on security requirements transparent, risk-based, and not overly prescriptive?
  - Do local laws and policies on law enforcement access to data avoid technology-specific mandates or other barriers to the supply of security products and services?
  - Are copyright laws or regulations in place that are consistent with international standards to protect cloud service providers?
  - Are copyright laws or regulations effectively enforced and implemented?
  - Is there clear legal protection against misappropriation of trade secrets?
  - Is the law or regulation on trade secrets effectively enforced?
  - Is there clear legal protection against the circumvention of Technological Protection Measures?
  - Are laws or regulations on the circumvention of Technological Protection Measures effectively enforced?
  - Are there clear legal protections in place for software-implemented inventions?
  - Are laws or regulations on the protection of software-implemented inventions effectively implemented?

'Authority protection' is based on four equally weighted measures:

- Protection of essential services index (Source: National Cyber Security Index)
- Protection of digital services index (Source: National Cyber Security Index)
- Protection of personal data index (Source: National Cyber Security Index)
- E-identification and trust services index (Source: National Cyber Security Index)

'Regulatory cooperation' relates to government's cooperation between agencies, both locally and globally. It is based on three equally weighted measures:

- Contribution to global cyber index (Source: National Cyber Security Index)
- Global Cyber Cooperation Index (Source: ITU; calculated using 2018 Global Cyber Index value and 2015 proportion of cooperation pillar)
- A score out of seven of a series of questions regarding cyber laws and regulations (Source: BSA The Software Alliance and Galexia Cloud Computing Scorecard)
  - Are there laws or appropriate guidance containing specific security audit requirements for cloud service providers that take account of international practice?
  - Are international security standards, certification, and testing recognized as meeting local requirements?
  - Are arrangements in place for the cross-border exchange of data for law enforcement purposes that are transparent and fair?
  - Are international standards favoured over domestic standards?
  - Does the government participate in international standards setting process?
  - Are there cross-border data transfer requirements in place?
  - Are cross-border data transfers free from arbitrary, unjustifiable, or disproportionate restrictions, such as national or sector-specific data or server localization requirements?

Preparedness Index: the organisational preparedness pillar contains four equally weighted sub-pillars

Readiness to respond' relates to response team capabilities and active management of threats. It contains three equally weighted measures:

- Cyber incidents response index (Source: National Cyber Security Index)
- Fight against cybercrime index (Source: National Cyber Security Index)
- Global Cyber Technical Index (Source: ITU; calculated using 2018 Global Cyber Index value and 2015 proportion of technical pillar)

Planning, management and exercises' relates to planning for response, including crisis team and plan development, and participation in cyber exercises. It contains three equally weighted measures:

- Cyber crisis management index (Source: National Cyber Security Index)
- Military cyber operations index (Source: National Cyber Security Index)
- Global Cyber Capacity Building Index (Source: ITU; calculated using 2018 Global Cyber Index value and 2015 proportion of capacity building pillar)

'Preventative measures' relate to steps taken to secure online transactions. It contains one measure:

- The proportion of licensed software (Source: BSA The Software Alliance)

Education and R&D' relates to research into cyber, cyber-related education, and individual capability to deal with cyber threats. It contains three equally weighted measures:

- Education and professional development index (Source: National Cyber Security Index)
- Human Capital Index (Source: UN E-government Index)
- Training and education index (Source: IMD World Digital Competitiveness Ranking 2019, IMD)

Endnotes

Chapter 1

[1] Deloitte Access Economics 2017, Connected Small Business

[2] The World Bank 2016, Digital Connectivity Helping Drive Growth in East APAC, available at: https://www.worldbank.org/en/news/feature/2016/04/21/digital-connectivity-helping-drive-growth-in-east-asia-pacific-but-millions-are-left-offline

[3] Microsoft 2018, Cybersecurity threats to cost organisations in APAC US$1.75 trillion in economic losses, available at: https://news.microsoft.com/apac/2018/05/18/cybersecurity-threats-to-cost-organizations-in-asia-pacific-us1-75-trillion-in-economic-losses

[4] Australian Trade and Investment Commission 2016, Cyber Security US clusters

[5] HFW 2019, The rise of cybercrime in APAC and considerations for organisations operating in the region, available at: http://www.hfw.com/downloads/The-Rise-of-Cyber-Crime-in-Asia-Pacific-August-2019.pdf

[6] AustCyber, SCP – Chapter 1 – The global outlook for cyber security, <https://www.austcyber.com/resources/sector-competitiveness-plan/chapter1>

[7] The ASEAN Post 2018, Southeast Asia's cybersecurity an emerging concern, available at: https://theaseanpost.com/article/southeast-asias-cybersecurity-emerging-concern

[8] Mordor Intelligence 2017, APAC Cyber Security Market, available at: https://www.mordorintelligence.com/industry-reports/asia-pacific-cyber-security-market

[10] AustCyber 2019, Cyber Security Opportunities in the ASEAN Region

[11] Mordor Intelligence 2017, above n 18.

[12] AustCyber 2019, SCP Chapter 1 – The global outlook for cyber security, available at: https://www.austcyber.com/resources/sector-competitiveness-plan/chapter1

[13] Reuters Plus 2019, Cyber Security Market 2019, available at: https://www.reuters.com/brandfeatures/venture capital/article?id=102621

[14] AustCyber 2019, Cyber Security Opportunities in the ASEAN Region

[15] CSIRO 2018, Cyber security: A roadmap to enable growth opportunities for Australia

[16] World Economic Forum 2019, The Global Risks Report 2019, available at: <http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf>

[17] HFW 2019, The rise of cybercrime in APAC and considerations for organisations operating in the region, available at: http://www.hfw.com/downloads/The-Rise-of-Cyber-Crime-in-Asia-Pacific-August-2019.pdf

[18] Varonis 2019, 60 Must-Know Cybersecurity Statistics for 2019, available at: varonis.com/blog/cybersecurity-statistics/

[19] Accenture Security 2019, The cost of cybercrime, available at: <https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf#zoom=50>

[20] Marsh and McLennan Companies 2017, Cyber Risk in APAC

[21] Telstra 2019, Telstra Security Report 2019, available at: https://www.telstra.com.au/content/dam/shared-component-assets/tecom/campaigns/security-report/Telstra%20Security%20Report%202019%20(1).pdf

[22] Cisco 2019, Cisco visual networking index: Forecast and trends 2017-2022 White Paper, <https://www.cisco.com/c/en/us/solutions/collateral/service provider/visual-networking-index-vni/white-paper-c11-741490.html#_Toc532256798>

[23] Ibid.

[24] Statista 2019, E-commerce in Asia, <https://www.statista.com/outlook/243/101/ecommerce/asia?currency=usd>

[25] Ponemon Institute 2019, The cyber resilient organisation,

[26] Deloitte 2019, All together now: Third party governance and risk management

[27] The World Bank 2016, Listed domestic companies, total, <https://data.worldbank.org/indicator/CM.MKT.LDOM.NO>

[28] Deloitte, Global Industry Threat Assessment: A Comparison of Threats , Actors, and Tactics Across Multiple Sectors (2019)

[29] Microsoft 2018, Cybersecurity threats to cost organisations in APAC US$1.75 trillion in economic losses, available at: https://news.microsoft.com/apac/2018/05/18/cybersecurity-threats-to-cost-organizations-in-asia-pacific-us1-75-trillion-in-economic-losses/

[30] Accenture Security 2019, The cost of cybercrime, available at: https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf#zoom=50

[31] Deloitte 2016, Beneath the surface of a cyberattack: A deeper look at business impacts, available at: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us risk-beneath-the-surface-of-a-cyber-attack.pdf 32 VMware Carbon Black 2019, Global incident threat response report, https://www.carbonblack.com/global-incident-response-threat-report/april-2019/#form

Chapter 2

[1] South China Morning Post 2018, https://www.scmp.com/news/asia/southeast-asia/article/2140073/cybersecurity-threats-are-rise-thailand

[2] AusCert 2019, https://www.auscert.org.au/our-culture/

[3] Australian Cyber Security Centre 2017, Threat report https://www.cyber.gov.au/sites/default/files/2019-03/ACSC_Threat_Report_2017.pdf

[4] CSO 2019, Australian universities are the world's most frequently targeted, https://www.cso.com.au/article/667702/australian-universities-world-most-frequently-targeted/

[5] Australian Government Department of Education, Academic Centres of Cyber Security Excellence (ACCSE) 2019, https://www.education.gov.au/academic-centres-cyber-security-excellence-accse

[6] Hays 2019, Cyber security talent report: Addressing the skills gap, https://www.hays.com.au/cs/groups/hays_common/@au/@content/documents/webassets/hays_2051431.pdf

[7] AustCyber 2018, Australia's Cyber Security Sector Competitiveness Plan 2018, https://www.austcyber.com/tools-and-resources/sector-competitiveness-plan-2018

[8] Spencer, L. 2018, $17M deal sees VMware bolster the ATO's cloud program, https://www.arnnet.com.au/article/633042/17m-deal-sees-vmware-bolster-ato-cloud-program/

[9] Cybersecurity Agency of Singapore 2019, https://www.csa.gov.sg/

[10] Cybersecurity Agency of Singapore 2019, Co-innovation and Development Proof-of-Concept Funding Scheme, https://www.csa.gov.sg/programmes/proof-of-concept-scheme

[11] Singapore Business Review 2019, Singapore ranks 10th in global cybersecurity: study, https://sbr.com.sg/information-technology/news/singapore-ranks-10th-in-global-cybersecurity-study

[12] Henderson, J. 2019, Singapore Airlines enhances employee experience through Vmware, https://sg.channelasia.tech/article/666432/singapore-airlines-enhances-employee-experience-through-vmware/

Chapter 3

[1] Deloitte 2019, The future of cyber survey 2019: Cyber everywhere. Succeed anywhere, available at: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-the-future-of-cyber-survey.pdf

[2] International Data Corporation, Security Solution Revenues in Asia/Pacific excluding Japan Will Reach USD 28.2 Billion by 2022, IDC Reports (09 April 2019) IDC https://www.idc.com/getdoc.jsp?containerId=prAP45005719.

[3] Deloitte, Cyber Regulation in APAC: How financial institutions can craft a clear strategy in a diverse region (2017) https://www2.deloitte.com/bd/en/pages/financial-services/articles/gx-cyber-regulation-asia-pacific.html.

[4] United Nations, UN E-Government Survey (2018) https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2018>.

[5] Deloitte, Building Trust Across Cultures: Privacy and Data Protection (2017), https://www2.deloitte.com/au/en/pages/risk/articles/building-trust-across-cultures.html.

[6] March & McLennan Companies, Cyber Risk in Asia-Pacific: the case for greater transparency (2017), https://www.marsh.com/my/insights/research/cyber-risk-in-asia-pacific-the-case-for-greater-transparency.html.

[7] Asia-Pacific Economic Cooperation, APEC Privacy Framework (2015), https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015).

[8] Deloitte & World Economic Forum, The Next Generation of Data-Sharing in Financial Services: Using Privacy Enhancing Techniques to Unlock New Value (2019), https://www2.deloitte.com/global/en/pages/financial-services/articles/the-next-generation-of-data-sharing-in-financial-services.html.

[9] Holman Fenwick Willan, The Rise of Cybercrime in APAC and Considerations for Organisations Operating in that Region (2019), http://www.hfw.com/downloads/The-Rise-of-Cyber-Crime-in-Asia-Pacific-August-2019.pdf.

[10] European Cybersecurity Forum, CTBERSEC 2018 Recommendations and Key Takeaways (2018), https://cybersecforum.eu/media/CSEU18_recommendations.pdf.

[11] Australian Bureau of Statistics, Characteristics of Australian Businesses, 2016-17, cat. no. 8167 (16 August 2018).

[12] Australian Government Attorney-General's Department, Protective Security Policy Framework (2018) https://www.protectivesecurity.gov.au/sites/default/files/pspf-govsec-06-contracted-goods-service-providers.pdf.

[13] Manushya, Thailand's Cybersecurity Act: Towards a Human-Centred ACT Protecting Online Freedom and Privacy, While Tackling Cyber Threats (2019).

[14] The Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth) (Austl.).

[15] Rahmansyah, D & Tahir, S, Indonesia: Data Protection Rules And Principles In Indonesia (29 January 2019) Mondaq http://www.mondaq.com/x/776534/data+protection/Data+Protection+in+Indonesia+Processing+Requirements.

[16] Personal Data Protection Commission Singapore, Overview (7 August 2018), Legislation and Guidelines https://www.pdpc.gov.sg/Legislation-and-Guidelines/Personal-Data-Protection-Act-Overview.

[17] ISC 2019, Strategies for building and growing strong cybersecurity teams: cybersecurity workforce study, https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=D087F6468B4991E0BEFFC017BC1ADF59CD5A2EF7

[18] Hays 2019, Cyber security talent report: Addressing the skills gap, https://www.hays.com.au/cs/groups/hays_common/@au/@content/documents/webassets/hays_2051431.pdf

[19] AustCyber 2019, SCP – Chapter 3 – The challenge: Australia needs to fill the workforce gap, remove startup barriers and strengthen research and development, https://www.austcyber.com/resources/sector-competitiveness-plan/chapter3

[20] Smart Nation Singapore, Smart Nation Scholarship, https://www.smartnation.sg/resources/smart-nation-scholarship

[21] Deloitte, Deloitte's Cyber Risk capabilities Cyber Strategy, Secure, Vigilant, and Resilient (2017), https://www2.deloitte.com/content/dam/Deloitte/at/Documents/risk/cyber-risk/Deloitte-Cyber-Risk-Capabilities-Broschuere.pdf.

[22] Deloitte, Cyber Regulation in Asia Pacific (2017), https://www2.deloitte.com/au/en/pages/financial-services/articles/cyber-regulation-asia-pacific.html.

[23] VMware, Core Principles of Cyber Hygiene in a World of Cloud and Mobility (2017), https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/vmware-core-principles-cyber-hygiene-whitepaper.pdf.

[24] Vincentis, M., Micro-Segmentation for Dummies (John Wiley & Sons, Inc., 2nd VMware Special Edition, 2017).

[25] VMware, What is Micro-Segmentation? https://www.vmware.com/topics/glossary/content/micro-segmentation.

Limitation of our work

General use restriction

This report is prepared solely for the use of VMware International Unlimited Company. This report is not intended to and should not be used or relied upon by anyone else and we accept no duty of care to any other person or entity. The report has been prepared for the purpose of examining and communicating the costs of and preparedness for cyber across selected countries in the Asia Pacific Region. You should not refer to or use our name or the advice for any other purpose.

Deloitte.

Deloitte Access Economics is Australia's pre-eminent economics advisory practice and a member of Deloitte's global economics group. For more information, please visit our website: www.deloitte.com/au/deloitte-access-economics

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities. DTTL (also referred to as "Deloitte Global") and each of its member firms and their affiliated entities are legally separate and independent entities. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories serves four out of five Fortune Global 500®companies. Learn how Deloitte's approximately 286,000 people make an impact that matters at www.deloitte.com.

Deloitte APAC
Deloitte APAC Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte APAC Limited and their related entities provide services in Australia, Brunei Darussalam, Cambodia, East Timor, Federated States of Micronesia, Guam, Indonesia, Japan, Laos, Malaysia, Mongolia, Myanmar, New Zealand, Palau, Papua New Guinea, Singapore, Thailand, The Marshall Islands, The Northern Mariana Islands, The People's Republic of China (incl. Hong Kong SAR and Macau SAR), The Philippines and Vietnam, in each of which operations are conducted by separate and independent legal entities.

Deloitte Australia
In Australia, the Deloitte Network member is the Australian partnership of Deloitte Touche Tohmatsu. As one of Australia's leading professional services firms. Deloitte Touche Tohmatsu and its affiliates provide audit, tax, consulting, and financial advisory services through approximately 8000 people across the country. Focused on the creation of value and growth, and known as an employer of choice for innovative human resources programs, we are dedicated to helping our clients and our people excel. For more information, please visit our web site at https://www2.deloitte.com/au/en.html.

Liability limited by a scheme approved under Professional Standards Legislation.
Member of Deloitte APAC Limited and the Deloitte Network.

©2019 Deloitte Access Economics. Deloitte Touche Tohmatsu