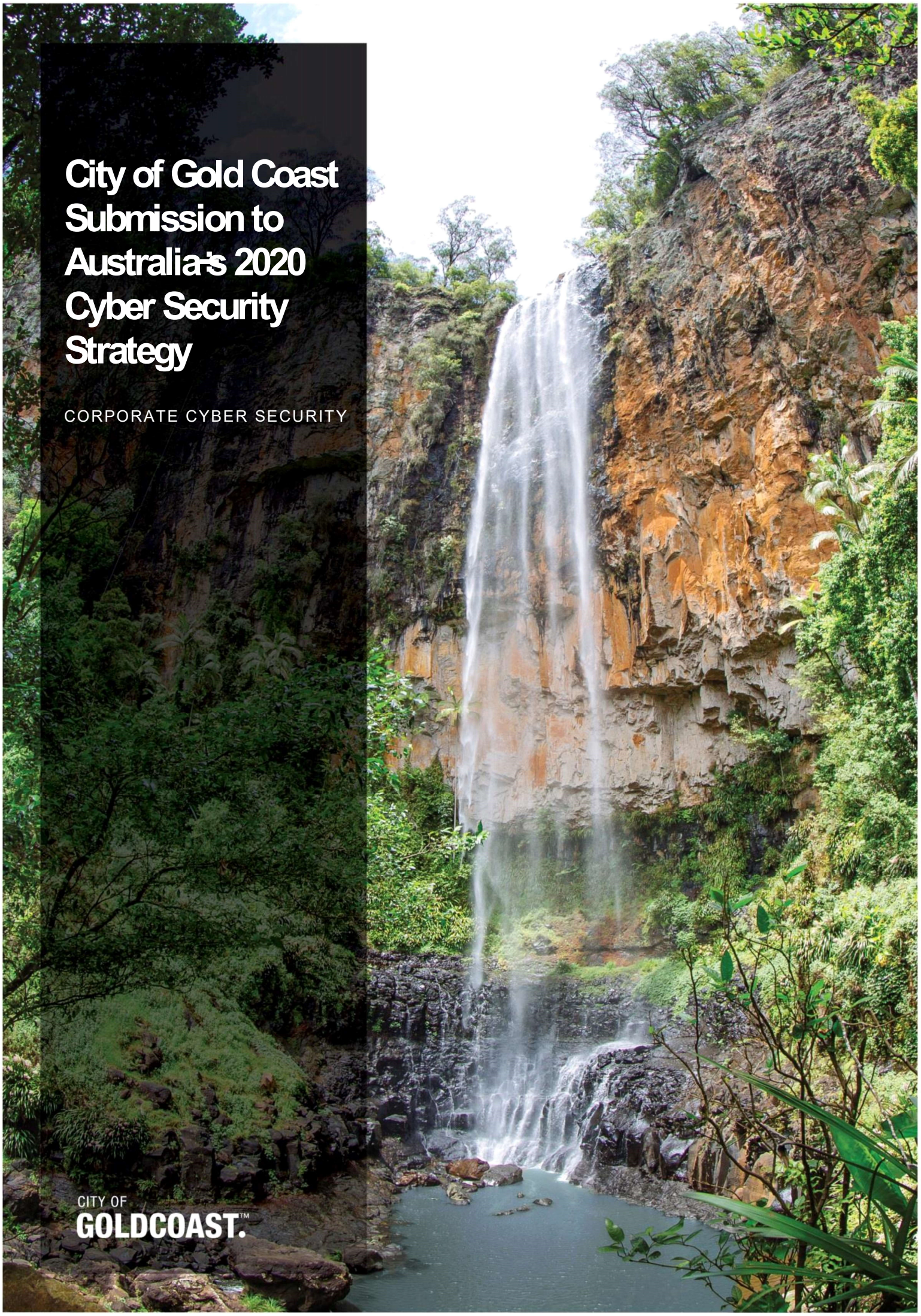
City of Gold Coast Submission to Australia's 2020 Cyber Security Strategy

CORPORATE CYBER SECURITY



CITY OF GOLDCOAST.™

Table of Contents

Introduction **3**
Summary **3**
Submission **4**

Introduction

The City of Gold Coast Submission to Australia's 2020 Cyber Security Strategy has been co-written by:

Matthew Walker CISSP
Glen Strickland CISSP SCCISP
Craig Blackwood CISM
Rhys Weightman

Summary

The co-writers of this submission have over 50 years' experience in cyber security spanning multiple countries working within industry verticals including Defence, Federal, State and Local Government, and energy utility sector. The City of Gold Coast (COGC) welcomes the opportunity to provide comment and feedback on the Department of Home Affairs, Australia's 2020 Cyber Security Strategy.

Matthew Walker
Executive Coordinator Cyber Security
Organisational Services
City of Gold Coast

[redacted]
PO Box 5042 Gold Coast Mail Centre Qld 9729
cityofgoldcoast.com.au

CITY OF GOLDCOAST.

Submission

1. What is your view of the cyber threat environment? What threats should Government be focusing on?

Response

The cyber threat environment is complex and ever-changing landscape for government, large, medium and small business, and citizens alike. Governments and Large business have legislation, regulation and frameworks to guide and ensure the security of the organisation.
However, small to medium sized business (SME) and the ordinary Australia citizen have limited funds, time knowledge and general ability to secure their data, information and privacy against the threats being discussed.

Based on 2020 Strategy figures people, "14% of Australians say they haven't taken any steps to protect themselves online"; and "$2.3 billion was stolen by cyber criminals from Australian consumers in 2017" this is the equivalent of $94 per citizen, however if only the 14% were subject to theft then only $323 million would be stolen.
At face value, these figures provide solid evidence that even though more than 86% of Australians take steps to protect themselves online, they are ill prepared or skilled to protect themselves.

The problem is exacerbated due to the nature of cybersecurity being a diverse and fluid target, where even the largest of organisations and government departments succumb to threat actors.

Government will need to take into account:

a) The majority of the Australian populous not having the skills needed to ensure the security of their data, information and privacy.
b) small to medium sized business may also be in the same predicament but now have to worry not only for their individual and staff data, but also of any customer data that they may collect or inadvertently obtain,
c) cyber security education and awareness (spam, phishing, etc.)
d) cyber skilled workers (basic security skills taught)
e) cyber security workers (specialised in cyber security domains)
f) cyber security information sharing and resources
g) complexity of cyber security
h) national security and defence
i) economic security and defence
j) intellectual property theft
k) supply chain risk

This must be a balanced approach with ensuring that government does not establish an environment of far reaching powers of surveillance, control and manipulation of the Australian citizens in the guise of protecting Australia and its people.

2. Do you agree with our understanding of who is responsible for managing cyber risks in the economy?

Response

COGC agrees in principle with your understanding of who is responsible for managing cyber risks in the federal and state economy and would welcome further elaboration and discussion on the responsibility for managing cyber risks in the local economy.

3. Do you think the way these responsibilities are currently allocated is right? What changes should we consider?

Response

COGC considers that the current allocation of responsibilities is ineffective and needs to be revised. Government should look to local government (where possible) to assist with managing cyber security risks in the local economy.

Local Governments could be utilised to engage with their ratepayers and constituents in cyber security awareness and education. Federally funded, Local Government managed and run collaboration hubs and information sharing resources (via established services e.g. libraries) to assist the public would assist in reducing the financial losses caused by cyber security theft.

4. What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?

Response

Government should take an active lead in addressing the most serious threats to Australian institutes and businesses, defending the Nations interests and economy. Government must update current legislation to encompass the modern internet paradigm, also ensuring that bilateral agreements are established with countries to assist in enacting cybersecurity on a global scale.

Government also needs to establish a simplified framework that can be used across organisations that can be used with most of the security frameworks and control standards.
Large Australian critical infrastructure organisations such as The Australian Energy Market Operator (AEMO) have already developed the AESCSF Framework and resources which leverages the US Department of Energy's Cybersecurity Capability Maturity Model (ES-C2M2) and the NIST CSF and references global best practice control standards.

Using a simplified cyber security framework such as one based upon the NIST CSF, will allow SME's to implement security in a simple and pragmatic approach. This can be used to align Australian-specific control references, such as the ACSC Essential 8 Strategies to Mitigate Cyber Security Incidents, the Australian Privacy Principles, and the Notifiable Data Breaches scheme (NDB).

Government must ensure the Cyber Security message is received by all organisations. This can be achieved using a multi targeted approach.

1. Legislation – Enforce cybersecurity on All large organisations causing a trickle-down effect, to SME's and Citizens alike
2. Awareness – Targeted media campaigns discussing the ramifications of cyber security theft the cost to the economy etc.
3. Education
    a. K-12 kids are taught cyber security basics, including bullying, privacy etc.
    b. TAFE / Community Colleges – Grass-roots Cyber Security technical skills
    c. 3rd party Security Training – Certification in Cyber Security domains, technical skills, governance and expertise
    d. University – Research and Degree level Cyber Security skills and expertise

Government must also establish a Whole of Australia mechanism to recruit, train and retain skilled resources in cyber security. Government could look at similar programs overseas and establish a suitable program in Australia.

Cyber security technical training could be established at TAFE / Community Colleges with internships and apprenticeships at supporting establishments including Local and State Governments. This could be paid for by the Government and repaid in a Return Of Service Obligation similar to existing Defence Services.

For degree and doctorate education and research, Australian Universities could partner with Government and offer cyber security masters, doctorates and degrees courses in a program similar to the United States of America CyberCorps® – Scholarship for Service program.

> *CyberCorps® - Scholarship For Service (SFS) is a unique program designed to recruit and train the next generation of information technology professionals, industrial control system security professionals, and security managers to meet the needs of the cybersecurity mission for Federal, State, local, and tribal governments. This program provides scholarships for up to 3 years of support for cybersecurity undergraduate and graduate (MS or PhD) education.*

A dedicated Cyber Security organisation must be a defensive organisation and should be an arm of the Department of Defence ensuring independence from influence of Government and Intelligence services. Oversight of the organisation will need to ensure that its remit is the defending the Nation and its Interests.

5. How can Government maintain trust from the Australian community when using its cyber security capabilities?

Response

Cyber security capabilities should be established in a dedicated Cyber Security organisation which must be a defensive organisation within the Department of Defence ensuring independence from influence of Government and Intelligence services. Oversight of the organisation will need to ensure that its remit is the defending the Nation and its Interests.

6. What customer protections should apply to the security of cyber goods and services?

Response

The statement “The variability in the security of cyber goods and services raises the question whether it is reasonable to expect providers to do more to protect their customers. Adding to this is the question of whether a purchaser is adequately equipped to protect themselves. It may indicate that strengthened protections are not feasible in some cases because they would impair the operation of a product or make it cost prohibitive This suggests a choice been potentially preventing consumers from accessing products that expose them to a high degree of risk, and allowing a consumer to accept this risk if they believe it is outweighed by the benefit the product brings” raises ethical questions on whether a good or service may restricted to a consumer based upon the degree of risk.

If we take the analogy of vehicle safety as a comparison; although we have the ANCAP safety rating where top safety rated cars attain a 5-star rating, whereas cars not achieving this level of safety are rated lower. The consumer, however, is not restricted from purchasing a 3 or 4-star ANCAP rated vehicle.
The consumer is now educated enough by media and vehicle manufacturers that the higher the star the safer the vehicle and is supported in that vehicles must now meet a regulatory standard safety rating before it can be sold to the Australian consumer.

Likewise, consumers are now being educated via friends, media and government and financial services providers on the purchase of goods and services from higher risk purchases and the mitigation of those risks. An example of this is the use of PayPal® for financial processing payments. PayPal Holdings Inc. operates a worldwide online payments system that supports online money transfers and serves as an electronic alternative to traditional paper methods like checks and money orders. The company operates as a payment processor for online vendors, auction sites, and many other commercial users, for which it charges a fee in exchange for benefits such as one-click transactions and password memory.

PayPal became the standard for consumer protection of high-risk transactions when there was no legislation or requirement for guidance.

Government has existing Australian Consumer Law to protect consumers. The Australian Consumer Law offers protection against faulty or unsafe products and services and unfair treatment from businesses.

How does Government enforce Consumer Law when the product or services is outside the jurisdiction of Australian Law? Achievability of enforcing this to international organisations is relatively low; however ensuring the financial security of funds for the procurement of the goods or services which are higher risk is achievable, by putting the onus of securing the transactions and refunds on the financial institution similar to the PayPal process.

7. What role can Government and industry play in supporting the cyber security of consumers?

Response

Government legislation containing direction for the protection of personal information, telecommunications, payments, banking and finance of consumers in a cyber context, would be beneficial. All are utilised in cybercrime.

8. How can Government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings?

Response

No response

9. Are there functions the Government currently performs that could be safely devolved to the private sector? What would the effect(s) be?

Response

No response

10. Is the regulatory environment for cyber security appropriate? Why or why not?

Response

No, the current regulatory environment is not appropriate. As cyber security professionals we routinely leverage other legislation to support advice/strategy. This requires knowledge of a range of Acts and regulations across privacy, public records, financial accountabilities etc., where applicable. Legislation containing direction for protection of personal information, telecommunications, payments, banking and finance etc. in a cyber context would be useful.

11. What specific market incentives or regulatory changes should Government consider?

Response

Enable fines for the loss or misuse of information. Include obligations to repair digital reputation, monitor and alert on further fraudulent identity use.

12. What needs to be done so that cyber security is 'built in' to digital goods and services?

Response

Cyber security regulation will increase pressure on manufacturers and sellers of digital goods and services. By way of example, the North American Electric Reliability Corporation (NERC) instituted the Critical Infrastructure Protection (CIP) cyber security regulations for power transmission and generation entities knowing that many current industrial control system manufacturers were not including secure by design elements in their operational technology systems. However, due to the regulatory requirement there is now market pressure for these manufacturers to improve their product design with additional security features to meet regulatory compliance.

Note that this approach may not work for all consumer products/services and may be better suited for some specific sectors, e.g. critical infrastructure.

13. How could we approach instilling better trust in ICT supply chains?

Response

The Federal Government should provide, as a service, a vetting and minimum compliance program for service providers and cloud providers which can be leveraged by public sector and private enterprise as part of their selection process (see https://www.fedramp.gov).

14. How can Australian governments and private entities build a market of high quality cyber security professionals in Australia?

Response

Government must establish a Whole of Australia mechanism to recruit, train and retain skilled resources in cyber security. Government could look at similar programs overseas and establish a suitable program in Australia.

Cyber security technical training could be established at TAFE / Community Colleges with internships and apprenticeships at supporting establishments including Local and State Governments. This could be paid for by the Government and repaid in a Return Of Service Obligation similar to existing Defence Services.

For degree and doctorate education and research, Australian Universities could partner with Government and offer cyber security masters, doctorates and degrees courses in a program similar to the United States of America CyberCorps® – Scholarship for Service program.

> *CyberCorps® - Scholarship For Service (SFS) is a unique program designed to recruit and train the next generation of information technology professionals, industrial control system security professionals, and security managers to meet the needs of the cybersecurity mission for Federal, State, local, and tribal governments. This program provides scholarships for up to 3 years of support for cybersecurity undergraduate and graduate (MS or PhD) education.*

A dedicated Cyber Security organisation must be a defensive organisation should be an arm of the Department of Defence ensuring independence from influence of Government and Intelligence services. Oversight of the new organisation will need to ensure that its remit is the defending the Nation and its Interests.

15. Are there any barriers currently preventing the growth of the cyber insurance market in Australia? If so, how can they be addressed?

Response

No response

16. How can high-volume, low-sophistication malicious activity targeting Australia be reduced?

Response

A mechanism to share threat intel, as a service, and advise entities and users of malicious sites e.g. phishing and malware could be an opportunity. This would be most successful as a devolved service considering the palette for the Government Internet Gateway.

Information Sharing and Collaboration Hubs providing timely threat intelligence to government and private organisations alike. Collaboration hubs should be focused on real-time communication (I.e. chat) between security leaders and specialists who are defending Australian organisations. Real-time communication enables threat sharing, indicators of compromise sharing, and exchange of information which improves the security posture of all participating entities.

17. What changes can Government make to create a hostile environment for malicious cyber actors?

Response

Domain take downs are slow and should be streamlined and accelerated. Reducing the effort to 'advise malicious activity' will reduce the effectiveness of high-volume attacks.

18. How can governments and private entities better proactively identify and remediate cyber risks on essential private networks?

Response

A mechanism to share threat intelligence, indicators of compromise, and malware information, as a service, to essential private network operators.

19. What private networks should be considered critical systems that need stronger cyber defences?

Response

A simple definition of critical infrastructure that is easily accessible should be developed. Although this is partially included in the CIC's Critical Infrastructure Resilience Strategy (2015) the succinct list should include:

- Health
- Food
- Finance
- Water
- Telecommunications
- Safety
- Energy and utilities
- Manufacturing
- Government
- Transportation

20. What funding models should Government explore for any additional protections provided to the community?

Response

Government should be fully funding the appropriate department/agency tasked with establishing and managing the Cyber Security of Australia. Business value can be quantified using the same figures cited in determining the economic losses, cyber security theft etc.

21. What are the constraints to information sharing between Government and industry on cyber threats and vulnerabilities?

Response

The greatest constraint to information sharing between Government and industry is awareness. Although the Government is providing information sharing via multiple websites, via StaySmartOnline etc., it is not widely disseminated, and is not providing timely updates.

An additional constraint is that information and remediation activities has an assumed level of knowledge of technology and security, this can be a detriment to usage if the person is not fluent in the discussion, and will ultimately stop using the site due to being confused or frustrated with the technical language.

22. To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?

Response

Lack of cyber awareness is only one factor in driving poor consumer choices and/or market offerings. Other factors include:

- Denial - "It won't happen to me..."
- Not my problem - "If it happens to me the bank/financial organisation will refund me..."
- Cost
- Complexity

The average consumer wants solution or product that "just works.." i.e. minimal configuration and minimal complexity. Any amount of cyber awareness will not work if the only simple to secure and use product or service

being offered is priced out of reach of the average consumer. Even ecosystems such as Apple have services and product offerings that are relatively secure, due to its closed ecosystem. However, most consumers still do not know how to configure services within the offerings to ensure the security of their systems and data.

23. How can an increased consumer focus on cyber security benefit Australian businesses who create cyber secure products?

Response

No response

24. What are examples of best practice behaviour change campaigns or measures? How did they achieve scale and how were they evaluated?

Response

No response

25. Would you like to see cyber security features prioritised in products and services?

Response

Yes. Cyber security features are generally an afterthought and lower on the priority list, this lack of prioritisation diminishes the overall security of the product and service to the organisation and consumer's privacy and data security.

26. Is there anything else that Government should consider in developing Australia's 2020 Cyber Security Strategy?

Response

No response

FOR MORE INFORMATION

P 1300 GOLDCOAST (1300 465 326)
W cityofgoldcoast.com.au

CITY OF
GOLDCOAST™