TrustedImpact
PROTECTING DIGITAL

Australia's 2020 Cyber Security Strategy

Call for views

October 2019

TrustedImpact is delighted to send the following input and perspectives on the new 2020 Australian Cyber Security Strategy.

Context of this input:

The viewpoints in this document are grounded in a foundation of several thousand technical to non-technical cybersecurity consulting projects conducted for over 13 years and with nearly 300; large to small, Commercial and Government clients.

This input, reflects hands-on insight gained at 'the coal face' of a statistically significant cross-section of the Australian cyber security landscape, which is respectfully offered for consideration into the Cyber Security Strategy of 2020.

The following presents six (6) important perspectives that we believe are essential for the next Australian Cyber Security Strategy.

1. A holistic approach is essential, thus a Federal Government role is required.

Cybersecurity, similar in many respects to Occupational Health and Safety, requires a thoughtful and holistic approach that spans not just technology, but people, process, education, regulation, etc. For example, it requires key elements of:

- Rules / laws / standards to be defined (eg, Mandatory Notification),
- Positive rewards or negative penalties to (re)enforce adherence to these rules / laws / standards,
- Independent, unbiased assessment of compliance with those rules / laws / standards,
- A populous that understands and values the importance of the problem,
- Affordable and available tools, techniques, and skills that help identify, understand and mitigate the risk,
- Defined, established, and ingrained processes that operate as a 'normal course of business' for all organisations and individuals alike to undertake as basic cyber 'hygiene',
- Programs that establish not just 'awareness' of the problem, but help inform businesses, communities, and individuals on how to protect themselves.

The Federal Government is in the ONLY position to be able to pull together these fundamental building blocks, and the new Strategy is the mechanism to do so.

Furthermore, as noted by a recognised industry pundit, Bruce Schneier, "The market does not reward security and privacy" – to expect citizen privacy or security to come from the commercial world is naïve, and it must be set and reinforced at a Government level.

However, to enable this to occur, the Federal Government must recognise that Cyber is a "Leadership challenge".

2. Cyber is a 'LEADERSHIP' challenge.

The tone of any type of organisation is set at the top. This is where priorities are defined, resources are aligned and progress is monitored.

In our more secure clients, cyber is discussed and challenged at very senior levels and not (like many of our less secure clients) relegated to a junior staff or embedded somewhere deep in an information technology department.

Toby Feakin aptly noted [here] in 2015, "[progress] requires a prime minister who will be prepared to champion the issue and spend some time talking about it with those that can make a difference".

The 2020 Cyber Strategy requires Government, Business and Community leaders to take a leadership stance to help champion the cause against a common enemy. We note the progress against Action #2, (pg 22 of the call for views) which woefully highlights this shortcoming.

Leaders do not need to be experts – they simply need to step up to leadership challenge that has been called by some [here] as 'the greatest threat to every company in the world... one of the biggest problems with mankind... and **the greatest transfer of economic wealth in history**".

ALL statistics agree that cyber security is one of our country's greatest challenges. Yet, if Government continues to de-prioritise or de-emphasise this issue, we will experience greater levels of compromise, and conversely, see the productivity benefits of the connected digital world pass Australia by in the next decade. Specific recommendations include:

- The PM should be seen to raise the issue of cyber and engage in discussions with other Government Leaders, Busienss Leaders, and Community Leaders – cyber security is an issue that affects all aspects of the populous.
- Federal Government should assign clear responsibility at a senior Ministerial level for Cyber alone – not just be one 'arrow in the quiver' of a portfolio responsibility.
- The Government "CISO" role (ie, held previously by Alistair MacGibbon) should be filled and be publicly heralded with a clear remit from the PM and Minister for Cyber.
- Round tables should be established to involve not just the ASX 10 (as were the majority of the small number of business 'round tables'), but involve other organisations and community leaders.

3. Measurement is fundamental.

The old adage "you can't improve, what you can't measure" rings true with respect to our Country's inability to describe and measure the threat of cybersecurity OR the opportunity to get it right (in terms of productivity and growth in relation to digital enablement).

The Federal Government is uniquely positioned to clarify the size and scale of the problem. However, this is woefully lacking. Nearly every statistic in the 'call for views' document (ie pg 7) is from an American-based product-oriented company, with a distinct commercial bias or conflict.

The simple fact that the 'call for views' document asks the question "what is your view of the cyber threat environment" highlights the fundamental problem. The federal government, ACSC, and strategy must establish the need for facts and statistics, not rhetoric.

Positive progress was made with the OAIC reporting of notifiable data breaches. This type of information is needed to understand whether progress is being made. It should be increased and extended to other aspects of cybersecurity (such as threats, volumes of threats, etc.). However, we note that the OAIC will be reducing the frequency of reporting – another example of the 'de-prioritisation' of cyber at Federal levels. Specific recommendations include:

- Key measures should be established to quantify the size, scale, and impact of cyber
- Mechanisms must be established to capture data that will reflect size, scale and impact of cyber
- Measures must be published frequently, with a) specific 'root cause' analysis behind what is impacting the measures, and b) with specific actions that other Governments (state or local), Businesses, Communities, and Individuals can take positively influence the measures and demonstrate progress

4. Cyber-related activities at the Federal, State and Local levels are duplicating effort, sub-optimising the outcome and wasting taxpayer funds.

For example, in just the small area of cybersecurity standards and frameworks, there are multiple frameworks at all levels of Government (eg the ISM versus the Victorian VPDSF). The result? Redundant and wasted effort to develop and maintain these individual frameworks at different levels and considerably greater effort required by those having to align with multiple, but slightly different frameworks. With limited resources to mitigate the risk of cyber security, we need less redundant work and more focus on improving the country's risk posture. Specific recommendations include:

- There must be a 'lead' organisation to take responsibility to 'harmonise' across different levels of government to minimise redundant activities. There are numerous examples ranging from frameworks through to education and awareness resources or tools. The list is extensive and, whilst the following statement is subjective, we are likely spending 10 times more in effort and cost for barely 1/10th of the impact in reduced risk.
- There must be recognition and incentives defined for the different levels of government to collaborate and coordinate. This requires budget to be allocated for meetings, workshops and integration activities, and

responsibility(ies) defined to achieve measurable outcomes relating to the area of coordination and collaboration.

5. It's time to mature beyond being 'AWARE', and the strategy must help Government, Businesses, and Communities to become 'INFORMED'.

In other words, many believe they are aware of the problem of cyber security, but most would not know what to do or how to go about minimising the risk of cyber.

Other countries (eg, the UK, and its Cyber Essentials), are making significant strides to help their constituencies become better at protecting themselves. The "Essential 8" approach is a great step in the right direction, but primarily focused on technical controls. We must embrace the fact that cyber risk is also very strongly a people-oriented issue and begin to arm our populous against these risks.

This issue resonates across most of our client base. Several years ago, our clients were getting compromised primarily due to technical vulnerabilities. Today, they face significant threats from people-based issues like Business Email Compromise and Malicious Ransomware. Specific recommendations include:

- Develop simple, easy to digest guides on the basics of cyber security,
- Advertise in a similar fashion as Occupational Health and Safety, or Road Safety to raise awareness and information across the populous,
- Engage trained practitioners to conduct workshops / town hall sessions to improve the levels of awareness and arm participants with techniques, tips and tools on how to better protect themselves,

6. Do not reinvent the ~~wheel~~ Federal Cyber Strategy.

How many individuals who were actively involved with the original 2015 Federal Cyber Strategy (advisory panel to staff), are going to be actively involved with this update? We suspect we know that answer.

The Federal Government risks wasting a significant amount of effort and time 'rehashing' issues that were already addressed, discussed or considered from the previous effort. Cyber isn't 'new' – the Federal Strategy should not be 'new' either. It's about learning what is working and doing more of it, and learning what isn't working, and attempting different approaches.

If you have any questions please contact:

Tom Crampton
Managing Director

TrustedImpact
Level 9, 22 Albert Road, South Melbourne VIC 3205
[redacted]

Appendix – Who is Trusted Impact?

In Summary

we're **independent** consultants – it's about **your** business and **your** success,

with a **singular focus** – information security is all we think about,

leveraging **experienced** professionals – credentials, not checklists.

We are **SPECIALISTS** in information security, not generalists in Information Technology, networking or other disciplines such as auditing.

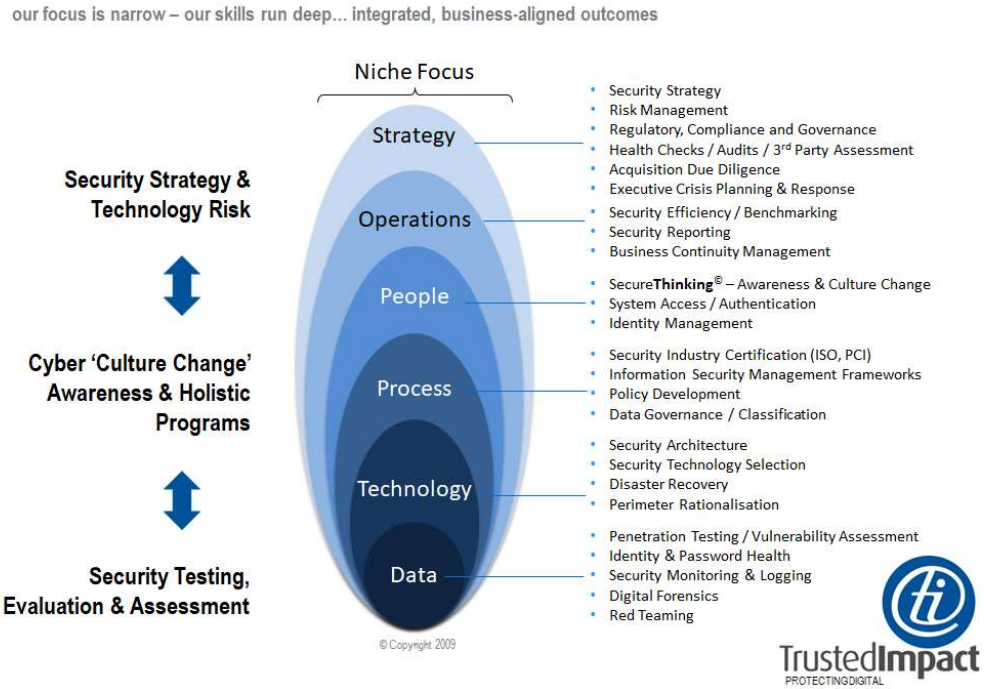
It is all we do, and because of that, we bring unparalleled experience and expertise to bear on our client's information security issues. With this focused approach, Trusted**Impact** has grown from a 'standing start' a decade ago to become one of Australia's leading firms in the industry. We're an independent consultancy focused on the best interests and objectives of our clients.

A focused business model

Information and the systems that process it are among the most valuable assets of any organisation. The adequate security of these assets is a fundamental necessity.

Trusted**Impact** helps enterprises improve performance by helping to identify and understand the important technology, people, and process trade-offs required to find a unique balance that reflects its strategy, operations, customers, suppliers and partners.

As illustrated in the following graphic, our business model uniquely combines the complementary security skills of cybersecurity strategy and risk, with cultural change management, to deep technical security expertise. Our focus is intentionally narrow, and our skills run deep… providing integrated, business-aligned outcomes in cybersecurity.



And blue-chip clients