Response to Call for Views on Strengthening Australia' Cyber Security Regulations and Incentives

August 2021

Introduction and Background

TechnologyOne welcomes the opportunity to provide its views in response to the Strengthening Australia's Cyber Security Regulations and Incentives paper.

TechnologyOne is an ASX 150 ERP provider, founded in Brisbane in 1987. Today, TechnologyOne operates across ANZ, AsiaPac and the UK.

TechnologyOne focuses on the vertical markets of Local Government, Higher Education, Government, Health and Community Services, Project, and Intensive Asset industries (utilities) and Fincorp.

TechnologyOne has evolved through successive generations of technology and is now one of a handful of providers of fully integrated Software as a Service ERP solutions in the world.

TechnologyOne has migrated well over half its customer base from on premise to SaaS, and more than two thirds of its state and Federal Government customer base.

We have more than 65 Federal Government agencies as clients ranging in size from very small to large, Tier 1 agencies.

SaaS provides many operational advantages to all our clients including allowing TechnologyOne to take over much of the management of these organisations' cyber security needs and compliance in relation to our applications. For example, we take responsibility for patching and pen testing to ensure compliance against the high standards of certification and assessment we have achieved.

As our software becomes more sophisticated, it becomes more difficult for customers to remain abreast of these obligations. By providing the software as a service, TechnologyOne is able to build security by design and use its scale to ensure security remains updated and compliant.

Technology One Limited | ABN 84 010 487 180
P. (07) 3167 7300 F. (07) 3167 7301 Level 11, 540 Wickham Street, FORTITUDE VALLEY QLD 4006 PO. Box 96, FORTITUDE VALLEY QLD 4006

TechnologyOne is acutely aware of the importance of cyber security and its responsibilities and the reality of the need to invest against an ever-evolving threat landscape.

TechnologyOne has placed cyber security at the centre of our planning and design of all services. We believe it is incumbent on us to be constantly lifting our cyber security posture on behalf of our customers.

We believe that trust is an inherent part of being a SaaS provider and that trust is earned not inherited from our customers. We have found that, in doing so, we are often leading our customers' own awareness of their cyber security risks and obligations as part of earning trust. This is true even of our Government customers who must comply with the most sophisticated set of security standards, requirements, and obligations.

In 2020, TechnologyOne achieved IRAP assessment as suitable for storing PROTECTED classified data. We subsequently lifted all Federal Government customers to that platform standard at no additional cost.

We applied the same architectural changes to our systems, and almost all the same processes and controls, to all customers in the course of achieving this level of assessment. We did so because it is our belief that the cyber security risk is not confined to Government, and nor should be the protections.

TechnologyOne has continues to develop its roadmap to invest in further lifting it security posture. We believe cyber security must be treated as a race without end. This represents a considerable cost to the business, but we continue to regard the duty to continually lift the bar on security as a cost of doing business for a service provider such as TechnologyOne. We note this is not yet a universally accepted position among our peers and competitors.

Our insights into the attitudes of our clients to this investment and to how they value the security embedded in our services provides, we submit, is a valuable insight into the challenges of lifting the cyber security posture of all Australian enterprises and therefore germane to this discussion paper.

Market Failure and Market Signals - Is Regulation Appropriate?

As a matter of principle, effective regulation serves to address points where markets fail to provide price signals that ensure conduct consistent with necessary market, social and/or national outcomes.

TechnologyOne supports the reasoning in the discussion paper that identified points where markets fail to that drive necessary cyber security responses and investments should underpin regulatory initiatives.

There are several points of market failure in cyber security, some of which are identified in the paper, some of which that TechnologyOne believes require further unpacking,

Technology One Limited | ABN 84 010 487 180
P. (07) 3167 7300 F. (07) 3167 7301 Level 11, 540 Wickham Street, FORTITUDE VALLEY QLD 4006 PO. Box 96, FORTITUDE VALLEY QLD 4006

One identified is that the cost of risk does not necessarily fall on those accepting the risk. For example, circumstances where the cost of a breach by a business is passed downstream to consumers.

Information asymmetry, where sellers are more informed than buyers, means there is often no premium for more secure services. This in turn creates an incentive for cost shifting to be unaddressed.

In addition, we submit there are at least three other related points of market failure that must be considered.

- Businesses are unwilling participants in the cyber-crime market. This is an asymmetrical market by its nature. There is competition between information systems owners and those who seek to access those systems. However, cyber security is not core business for those engaged in legitimate commerce. It is, however, the only business for those in the business of monetising for cyber insecurity
- Increasing involvement of state actors with mixed motives. E.g., economic disruption for reasons of ideology or political advantage, not financial gain. This means businesses acting to protect their commercial interests, and even those of downstream customers, might define the threat too narrowly to protect broader social and national interests.
- The investment capacity of specialist bad actors, especially state actors that do not require a commercial return, far outstrips the capacity of all but the very largest business and public sector organisations to invest in response.

We submit the Government has a legitimate interest in regulation to address market failures that causes cost to be transferred e.g., from a party who has a security failure to a downstream customer AND to protect the national interest and maintain national economic and social continuity.

However, we believe the regulatory requirements cannot be imposed only on large private organisations, as proposed in the paper. The interconnectedness of organisations of all sizes means that “weakest link” attacks represent a very real danger. They are only likely to increase if larger targets are hardened.

This is especially true of state actors motivated not to seek commercial targets but to create social and economic disruption.

We acknowledge that this creates a significant challenge for regulation as the cost of regulation has the potential to distort markets.

The uneven level of awareness and understanding TechnologyOne has observed even in our Government client base, however, gives us concern about risks of a “top of town” only approach. We propose below what we believe are approaches that might balance these competing interests.

Technology One Limited | ABN 84 010 487 180
P. (07) 3167 7300 F. (07) 3167 7301 Level 11, 540 Wickham Street, FORTITUDE VALLEY QLD 4006 PO. Box 96, FORTITUDE VALLEY QLD 4006

Our Experiences and Client Insights

As discussed above, TechnologyOne has lifted all clients' cyber security posture as it has invested in improving its core cyber security capability. The most high-profile example of this was the decision in 2020 to lift all Federal Government agencies to the PROTECTED-assessed service at no additional cost.

TechnologyOne informed Federal Government SaaS customers in advance, due to the significance of the PROTECTED assessment.

While TechnologyOne was clear that is did not seek to recover its sunk costs in achieving PROTECTED through increased prices, the process of rolling out the information about this impending uplift provided concerning insights into how cyber security is understood and managed by some agencies. This included larger agencies.

Even among Government customers, there was not a universal welcoming of what was, in effect, a no-cost security uplift. Several agencies questioned whether they needed to be moved to the more secure platform, even though TechnologyOne was at pains to ensure it came at no cost, minimal disruption (the process was usually completed without the customer even noticing) and no loss of application functionality.

Some of this resistance was based on a failure to understand modern SaaS technology. This was evident across business areas, security, and IT teams. Some seemed to be simply a resistance to any change, even a change that was all benefit and no cost.

The mixed reaction also indicates that cyber security is not universally understood for what it is: a cost of doing business that cannot be ignored, and a race without end that requires specialised assistance.

We submit these insights show how far there is to go before cyber security is afforded the priority it requires in the face of the material and universal threat of cyber crime. They also show that it requires a greater direction from senior executives who sit above functional business, IT and Security units.

With this in mind, TechnologyOne submits Government action toward increased regulation of cyber security measures must seek to achieve a fundamental shift in mindset across the entire business and public sector agency community.

Solutions

Effective security is now beyond the reach of all but a very few government agencies or businesses. Even among large organisations, those with the most mature strategies are likely have a reason to specifically value security very highly because it goes to their core business, such as financial sector.

Technology One Limited | ABN 84 010 487 180
P. (07) 3167 7300 F. (07) 3167 7301 Level 11, 540 Wickham Street, FORTITUDE VALLEY QLD 4006 PO. Box 96, FORTITUDE VALLEY QLD 4006

As discussed above, however, the risk -- commercial and to the nation -- is spread across all sizes of organisations and the “weakest link” problem exacerbates this problem.

At-scale, as-a-service solutions to cyber security are therefore required such that advanced security solutions are priced within the reach of enterprises of all sizes.

The technology mega trends of cloud-based Infrastructure as a service and Software as a service have been driven by business benefits. That is, they are being driven by the commercial cost/price signals that businesses understand.

Fortunately, though, they can have the positive externality of both reducing costs and increasing the quality of security measures specifically.

That is, an improved cyber security posture can be a positive externality from investment in transformative technology that is supported by a core return on investment business case.

There is evidence that this relationship is increasingly understood and being factored into decision making. This was a finding of a research report commissioned by TechnologyOne from Insight Economics and IBRS, *The Economic Impact of Software as a Service in Australia,* released in August 2021.

The report found the potential for substantial benefits both to individual enterprises and to the nation from the more rapid uptake of SaaS technologies in the form of reduced costs and subsequent economic flow-on effects. In a series of case studies and an extensive literature review, it found costs savings and the opportunity for business process transformation were the primary motivators for organisations investing in these technologies.

However, it also found businesses and agencies moving to SaaS reported both reduced expenditure on cyber security (4-8 percent reductions) and improved security performance due to regular patching and updates. The report authors reported improving cyber security performance without increasing expenditure on security was a major factor in organisations deciding to move to SaaS.[1]

Improving understanding of the potential for a “win-win” investment in business technology solutions should be an objective of new initiatives, including new regulation.

Similarly, increasing understanding of the increasing cost and complexity of attempting to remain up to date with security challenges should be an objective.

The Federal Government has provided such clear advice to its own community of agencies.

The ACSC’s Anatomy of a Cloud Assessment and Authorisation advises agencies that they should consider first the risk of NOT using a cloud provider when considering a move to a cloud service.

> *Organisations who manage and secure their own Information Technology (IT) infrastructure, such as an on-premise environment, need to consider as part of their risk assessment of cloud computing, the risks of not transitioning to cloud computing.*
>
> *An organisation who owns and manages its own IT infrastructure is responsible for securing all aspects of it, including achieving the desired security baseline, maintaining it and updating it as adversary tradecraft evolves; depending on the size*

[1] The economic impact of Software as a Service, IBRS and Insight Economics 2021 Page 53

Technology One Limited | ABN 84 010 487 180
P. (07) 3167 7300 F. (07) 3167 7301 Level 11, 540 Wickham Street, FORTITUDE VALLEY QLD 4006 PO. Box 96, FORTITUDE VALLEY QLD 4006

of the environment, this may necessitate significant effort and resources on behalf of the organisation to achieve this.

As part of an organisation's examination of cloud computing, it needs to consider its own capabilities to secure their systems and protect their information from current and future cyber threats. If an organisation's basic security practices such as patching, upgrading and system hardening are ineffective or inconsistent, cloud computing may provide significant security improvements. By transferring some security responsibilities to the CSP, an organisation can prioritise other, more specific security mitigations such as access control, authentication, and monitoring. In addition to transferring some security responsibilities, leveraging the advanced security technologies available from many CSPs can provide substantial cyber security improvements beyond what is feasible when an organisation owns and manages its own IT infrastructure.

This advice is equally applicable to private sector organisations as Government agencies. For Government agencies, though, it is supported by the force of the requirement for Government agencies to comply with the PSPF and ISM.

No such regulatory "stick" exists to encourage private industry to challenge itself with the same question about the capacity to protect on premise systems.

Proposed Regulatory Actions

As discussed above, TechnologyOne believes regulatory initiatives should be designed to address organisations of all sizes. They should also be aimed at addressing market failures by replicating price signals. Taken together, they should be both carrot and stick to minimise the cost of regulation.

We propose the following for consideration:

- A financial incentive for digital providers to invest in higher levels of security. Organisations that invest in achieving accreditations against security standards cannot recover this investment through premium pricing. This disincentive should be offset by a mechanism such as a small tax rebate against sales of products incorporating these accreditation investments.
- An incentive specifically related to annual new investment in cyber security uplift. This could possibly be modelled on the R&D Tax Incentive. Cyber security is a race without end that has been threat-led. Balancing this requires a device to encourage organisations to move beyond static measures such as accreditations. A financial incentive to reward constant investment is worth considering.
- Expanded mandatory reporting of cyber incidents. This should include ransomware events. The intention is not to name and shame, but to lift education and provide more visibility into the sources and motives of bad actors. Consequently, identities of organisations should not be revealed to encourage compliance. The anonymous publication of data about attacks will assist senior executives and boards to better understand the risks and threats.

Technology One Limited | ABN 84 010 487 180
P. (07) 3167 7300 F. (07) 3167 7301 Level 11, 540 Wickham Street, FORTITUDE VALLEY QLD 4006 PO. Box 96, FORTITUDE VALLEY QLD 4006

Contact

TechnologyOne is committed to engaging constructively in Government processes to develop ore effective cyber security policies and regulations.

For further information or discussion, please contact:

David Forman
Director, Federal Government Relations
[redacted]