technologyone
Transforming business, making life simple

Submission in Response to

5 Year Productivity Inquiry: Australia's data and digital dividend

Interim Report

September 2022

technologyonecorp.com

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

Innovation, Productivity and Core Systems

Retina Visions is a technology start-up business founded in 2016 to provide automated transport network condition assessments using machine learning and IP-based video input technology. It has deployed its technology in with local government customer by deploying inexpensive IP video cameras in the front of garbage trucks.

As these trucks traverse their regular routes, the cameras are continually capturing images of the pavements and surrounds. These data are analysed to triage the defects.

Retina Visions's service removes the need for councils to collect and manage data on the road service, allowing them to concentrate on repair and improvement of the assets.

TechnologyOne has partnered with Retina Visions to extend this further by fully automating the subsequent creation of work processes to manage the defect rectification process. TechnologyOne's core ERP system is fully accessible from any browser or any device using a browser. This means the triaged data from Retina Visions can be consumed directly into the TechnologyOne asset management system, initiating the creation of a work order. This work order is delivered by any mobile device to a work crew, with location and work instructions, including maps and photographs of the site. The crew can close the job and include images of the completed work.

One council deploying the integrated solution found benefits included:

- 20-40 percent reduction in customer calls
- Double the number of potholes being rectified

Potholes in road surfaces are one of the most common causes of residents contacting the local council. The cost of road maintenance is also one of the largest operational costs centres for local government.

This story is an example of two things. Innovation is facilitated by a modern, open, IP accessible information system at the core of the enterprise. In a previous generation of technologies, the integration requirements would have meant edge applications would have been expensive and slow to deploy, and would have been bespoke builds in each use instance. IP is a data format that can support any form of data, from text to video, allowing for great input flexibility. This lowered technological barrier to entry is facilitating opportunities for start-ups tht would never have existed a decade ago.

Secondly, while the end application may be eye-catching and ground-breaking, the direct integration into core systems is where there are often overlooked opportunities for big labor productivity gains are likely to be found.

In the Retina Vision/TechnologyOne example, the automated fault identification and triaging of defects is clearly transformative to the citizen experience as defects are reported more quickly.

However, the less visible process transformation is in the core business system, where defect rectification is initiated, tracked and closed. The earlier and more efficacious repair of the assets that is facilitated transform and automate the business processes to issue, execute and close work orders.

Introduction

TechnologyOne welcomes the opportunity to continue to participate in the Commission Five Year Productivity Inquiry.

The Commission's Second Interim Paper focuses on the role of technology in future national productivity performance. TechnologyOne agrees accelerating the diffusion of technology will be central to any successful program to lift the national productivity performance. Technology represents one of the few levers available to policy makers to create a step change in productivity performance.

In its previous submission and the supporting research report[i], TechnologyOne described how there is a transition underway from an own-operate model of business intelligence technologies to a consumption-based model. The new model is qualitatively different in productivity outcomes.

The transition is analogous to that experienced by music listeners over the recent decades., Music users once acquired individual recordings that were played on a device that was either so large it required listeners to sit in one room to listen to the recordings or, if it was portable, provided a diminished quality and still worked in only limited conditions.

Today, our consumption of music has been transformed. Modern technologies both liberate the recording from the medium, allowing access to almost any piece of music in any order one can imagine, and liberates its playing to any connected media device, at any time, at any place where there is wireless or fixed line access.

The same liberation is being experienced by productive applications. Applications are increasing allowing transactions to be initiated and completed at the edge of the network, as in the case study described above. Friction points that arose from the limitations of technology have become so embedded into business processes that they are barely recognised for what they are. But when the technology is changed, the opportunities for innovation and productivity unleashed are revolutionary.

In its paper, the Commission proposes several factors that could be inhibiting the more rapid adoption of digital technologies.

Several of these factors, in our submission, should not be barriers to the adoption of consumption-based software. Rather, the fact that they are proposed as constraining factors underlines that other factors, including several identified by the Commission, must be addressed.

Low awareness by management, transition costs, and uncertainty of benefits are, we believe, the biggest inhibitors to a more rapid digital uplift.

Policies should be considered to focus on these underlying inhibitors.

Inadequate Internet

TechnologyOne operates throughout Australia with a focus on the market verticals of Local Government, Education, Government, Health and Community Service and Asset Intensive Industries. Lack of Internet infrastructure is no longer a constraint for customers in any of these verticals gaining the full functionality of SaaS technologies.

Underlying infrastructure in the form of the NBN and 5G mobile networks are now so widely deployed as to be near ubiquitous. It is important to remember the rationale for the public

intervention to ensure the NBN provided universal connectivity was based in an expectation that emerging technologies, such as consumption-based information services, would be the foundation of future economic success, nationally and regionally, and social welfare and inclusion.

The convergence of communications software systems and networks to Internet Protocol over recent decades has allowed for greater interoperability, flexibility, resilience and robustness and has lowered bandwidth requirements for business applications. Applications are able run effectively even when there is some loss of data or network interruption. IP is inherently designed to operate over divergence paths and tolerate some packet loss.

The bandwidth required for an organisation to operate the TechnologyOne ERP SaaS suite is substantially less than for video conferencing, for example.

Further, the remote access technologies that allow transactions to move to the edge of the network and into the hands of mobile workforces, creating opportunities for business processes to be transformed and automated end-to-end, require relatively low wireless bandwidth, and can adapt to periods and locations where connectivity is interrupted.

Lack of Skills

SaaS technologies require different skills, but typically these are less specialised.

In the past, applications were bespoke implementations that differed in every customer's environment, which was, in turn, individual. Internal IT teams often had years of skills and understanding of these unique software deployments.

Tasks such as upgrading versions of software could be a major project that demanded additional IT resources and could amount to complete reimplementation of software, along with substantial change management and user training. Upgrades were therefore infrequent – usually years apart.

SaaS applications are consumed rather than owned and managed on premise and are typically upgraded much more regularly. The requirements on businesses are largely testing of new features and change management with users. The more often upgrades are taken, the more easily each new version is consumed.

This frequency and the immediacy with which upgrades and new features are deployed across the entire community of users of applications dramatically reduces the time to value for users.

Individuals who have in the past been employed to install and maintain software on premise can usually adapt their skills to the new tasks required to support organisations successfully consume and manage SaaS applications, and to projects configuring off the shelf software to deliver productivity enhancing workflow processes.

Security Concerns

It is now generally acknowledged that, aside from a small subset of highly sensitive data related to national security held by a small number of organisations, cloud-based data management is almost always associated with an improved cyber security posture.

Tasks such as patching and upgrading of software are basic requirements of good cyber security practice. However, time and again, even government agencies with mandatory patching compliance obligations have been found to struggle to stay up to date.

Cyber security can be seen as analogous to asymmetrical warfare. Typical organisations are primarily – and properly – concerned with conducting their core business. They are increasingly finding their resources are diverted to cyber defence, which for them is a cost centre.

Bad actors, however, are increasingly organised and specialised. They are able to avail themselves of "tool kits" for exploiting vulnerabilities in the information systems of their victims by accessing the Dark Web. These tool kits allow them to monetise illicit access to the networks of businesses and even individuals.

In other words, they are single purpose, for-profit businesses seeking out and exploiting underinvesting victims.

Some of the most serious cyber-related disruptions in recent years have resulted directly from failures in basic software management "hygiene" such as patching against known vulnerabilities, by organisations that have had insufficient focus on keeping their total system defences up to date.

In some cases, such as the National Health Service in the UK, major cyber security issues have resulted from a combination of old on-premise software – some so out of date that it is no longer supported by the manufacturer – and known vulnerabilities that have not been patched in the past and, in some cases, can no longer be fixed.[ii]

When consumption-based computing resource and software systems are adopted, managing hygiene and maintaining cyber security compliance obligations are responsibilities taken on by the service providers. Unlike individual organisations such as the NHS trusts, the SaaS providers can build the scale to resource this effectively. Providing secure, reliable service is their sole business and cyber security is a core business input cost.

SaaS applications are patched remotely on a regular frequency – monthly or even more often. In the event of an identified security vulnerability – such as so called zero-day events – patches are often provided as soon as they are made available. Situations such as that described related to the NHS cannot occur as software of that age would simply not be available for consumption.

Another benefit of SaaS software is that repairs and responses are implemented immediately to all customers. Again, many major cyber events in recent years have exploited a "long tail" of organisations that have not patched vulnerabilities long after patches were made available, either through lack of resources or awareness.

Of further concern is that, in TechnologyOne's experience, organisations very often are unable to identify the internal costs associated with their cyber security measures.

The SaaS research paper produced by IBRS and Insight Economics found businesses are increasingly adopting SaaS services in order to improve their cyber security posture while managing the growth in the increase of cyber budgets. [iii] Management that has not insisted on a proper accounting for cyber defence costs, or has not insisted on an honest audit of performance against modern cyber hygiene and performance standards is not in a position to make such as decision, however.

Cost and Legacy Systems

Understanding and managing the costs associated with adopting new, consumption-based technology models and retiring legacy systems presents barriers to change in several ways.

Firstly, there are legitimate budget challenges, particularly for larger organisations, because some legacy systems cannot be retired simultaneously with the commissioning of new systems.

Secondly, the business models supporting consumption-based hardware and software have been mixed, in that they include a call on capital budgets for implementation as well as an increase in recurrent spending. This can make it difficult to make meaningful cost comparisons and create confusion about the value of the change unless the decision makers understand they are not comparing like for like when comparing on premise to as-a-service.

Thirdly, there is often a misunderstanding of the range and full extent of savings that accrue from a move to SaaS because many of the costs of functions presently performed "in house" are not properly understood or recorded. An example of this is the cost of cyber security compliance discussed above.

Finally, there is often an empowered constituency inside organisations with a vested interest in arguing in favor of incremental technology investments in the form of internal IT teams and external businesses reliant on old approaches, due to simple resistance to change.

Transition Periods – Switching Costs, and Mixed Business Models

One of the challenges for larger organisations transitioning away from legacy technologies and applications is managing the period where both old and new systems are being maintained. This switching cost is associated with moving individual applications and with whole of business changes from "own-operate" to "consumption" technology models.

An example is an organisation moving one application from on premise or hosting infrastructure that cannot retire the cost associated with the supporting infrastructure because it is still required for other applications. The costs are not associated with the application no longer supported on premise, but may nonetheless still be incurred.

Organisations moving through this transition may face an extended period when ICT costs could be increased as new systems are installed over time and legacy systems are maintained in parallel. It is not unusual for organisations to be unable to transition all applications at the same time, either because of internal resources constraints in managing multiple processes simultaneously or because some legacy applications are unable to be transitioned.

For example, TechnologyOne has encountered situations where public agencies have a reliance on a very old software applications to support a specific function they provide, such as a licencing function. Off the shelf alternatives may require changes in business processes. Agencies will sometimes resist making these changes. This can mean these agencies extend or support for longer on-premise infrastructure and licences that once supported multiple applications, for only one or two old but highly specialised pieces of software.

This "double bubble" problem is exacerbated if there is up front capital investment required to implement the alternative SaaS application.

That is, SaaS applications are recurrent cost items once they are operational. But there is very often also a capital cost associated with the initial implementation of these systems, requiring a call on capital budgets as well.

This problem is exacerbated by the mixed business models on the technology supply side.

Many large software providers support an ecosystem of channel partners who maintain business lines both advising organisations on what software to buy, and separately implementing the software (often from these same vendors).

These business relationships are in many instances a legacy of the own-operate software marketing model. Software developers built sales channel networks with the local partners software buyers needed to install and manage software in their offices or data centres.

Over time, this has become such a large and lucrative industry that the relationships between the implementation partners and software vendors continue in an era when most of software vendors are seeking to transition to SaaS technologies that have quite different on-going support requirements.

Confusing the environment further is a tendency to conflate different X-as-a-Service technology under the single term “cloud”. Infrastructure-as-Service refers to the outsourcing of computing hardware. Software being run on such an outsourced computing environment is still usually owned and operated by the end user enterprise.

Software-as-a-Service incorporates the capital and maintenance costs of all the underlying infrastructure, and the development, maintenance, and support of the software.

There can also be human factors at play in organisations that have powerful and historically independent IT workforces. This can present as an internal constituency that is both resistant to change and has the power to slow transitions. This may be a factors in decisions to maintain bespoke applications.

These attitudes can arise from a combination of factors. In some cases, those who have worked with old applications for many years may be conservative and risk averse about emerging technology that is fundamentally different from what they understand and are comfortable with. TechnologyOne has also seen situations where IT teams trained in old applications may be motivated to slow change until they can find alternative employment or retire, rather than retrain.

Accelerating Uptake – Educating Management and Challenging Business Models

Initiatives to accelerate the diffusion of modern business intelligence systems to promote a national productivity uplift should take a focus on both supply and demand side measures.

On the demand side, many of the factors slowing the more rapid diffusion of modern, consumption-based information systems can be seen as the result of management not being sufficiently educated about technology to treat it as they would any other business input.

If the senior management of an organisation does not understand the qualitative differences between the underlying technologies and the productivity step change opportunity offered by a transition to a consumption model, it becomes much more likely an organisation will choose to make incremental investment in existing systems.

This understand requires a conceptual understanding of technology, not technical expertise per se.

By way of comparison, most management teams would readily understand the difference between the cost of buying and running a fleet of vehicles, with all the obligations to insure, maintain, register and provide fuel, against the cost of outsourcing or even the cost of catching public transport, where those costs are incorporated in the service costs. But few executives could so easily identify a list of costs associated with a technology choice.

Understanding these cost comparisons conceptually does not require a deep technical knowledge any more than understanding the comparable costs of transport requires a deep understanding of motor mechanics.

On the supply side, there is a case for action to encourage business models to be reconsidered.

TechnologyOne has recently responded to the switching costs challenges its customers face by developing subscription only pricing models where there is no separate implementation capital expense. In the same way as it embeds the cost of R&D into the annual subscription, the cost of implementation is treated as an input cost to the service, rather than a different transaction.

This flattens and simplifies the charges to the customer.

Were such a change to be driven across the industry, it would challenge the relationships between software providers and their partners.

The separation of software supply and implementation and support creates perverse and misaligned incentives on the supply side. Software implementation partners benefits from project budgets being extended, and for bespoke implementations, as these may require additional work whenever there is a software upgrades, work that is often provided by the implementation partners.

While the software provider might rely on the partner as a sales channel, its longer-term incentive is for the customer to have successfully deployed the solution.

A pricing model embedding implementation and upgrade costs aligns incentives of the software provider and its service partner. Both need to minimise costs and complexity to protect margins over time. The time to value for the customer is thereby reduced.

Recommendations

Governments can play a role as a technology user and buyer to encourage both supply and demand side change. Recommendations TechnologyOne made in its earlier submission to this inquiry seek to address both.

- Introduce a SaaS-First policy across Government.

The Cloud First policy adopted by governments around the world, starting more than a decade ago, had a powerful catalytic effect on the buying practices of government agencies, and encouraged broader change by example across the economy.

Requiring agencies to choose cloud infrastructure as a first choice shifted deep cultural conservatism and empowered public servants to make different decisions.

SaaS First is the evolution of Cloud First and would drive Government to keep pace with the changes in technology over the past 10 years. It would also drive a deeper understanding of the differences between various as-a-service offerings and support better cost-benefit models to support procurement decisions.

- Security standards

Governments should enforce strict requirements in agencies and sensitive sectors and communicate their own security standards and expectations to the market. This would encourage senior management in both their own agencies and the private sector to develop their own understanding and expectations.

The Information Security Manual is a comprehensive set of requirements applying to all Federal agencies. However, agencies continue to struggle to meet obligations such as compliance with the Essential Eight as a baseline for cyber resilience.[iv]

It is increasingly clear that modern, fit-for-purpose cyber security can only be delivered through scale solutions, such as through cloud-based technologies. Combined with a SaaS-first policy, this could drive a more rapid market transition to superior, SaaS cyber security solutions across government. This, in turn, could stimulate supply side investment, such as encouraging international cyber security providers to invest more heavily in Australia.

- Best-practice buying model

Governments can develop tools to properly capture the full costs and benefits of step change technology investment decision-making and make these available to the business community. This would support a SaaS First policy for Government agencies. Governments informed by better models can also more effectively use their buying power to drive creative supply-side pricing models, which will flow through to the private sector.

That is, government buyers can encourage vendors to propose pricing models that address the fiscal circumstances and the disincentive to investment in transformative technology created by the cost of retaining legacy systems in parallel as they are retired over time. Flattening the cost curve for government agencies can be the difference between incremental and transformation investment decisions by individual agencies.

Contact

TechnologyOne would welcome the opportunity to meet with the Commission to explore the issues raised in this submission or provide further information at the Commission's request.

Please contact

David Forman
Director of Government Relations

[i] The Economic Impact of Software as Service, IBRS and Insight Economics
[ii] https://www.digitalhealth.net/2019/04/outdated-software-leaves-nhs-vulnerable-to-cyber-attack-new-research-says/

[iii] https://www.cisolens.com/benchmark
[iv] Interim report on Key Financial Controls of Major Entities, ANAO, Auditor-General Report 32 2021-22