Submission by Department of the Prime Minister and Cabinet

CYBER SECURITY AND DIGITAL DELIVERY OF GOVERNMENT SERVICES

Overview

Opportunities

Our society is rapidly undergoing a digital transformation and our government services with it. We estimate that 90% of Australians are already online with that proportion continuing to grow. Similarly, 84% of Australian small and medium-sized businesses already have online presences, with half now receiving payments online.

As the Prime Minister said when he launched Australia's Cyber Security Strategy in April 2016, "there is no global institution or infrastructure more important to the future prosperity and freedom of our global community than the Internet itself." As the majority of Australian businesses have done, the Australian Government has embraced the opportunities the internet offers in the provision of services to the Australian people. This is being pursued through the Digital Transformation Agenda. But the potential of digital transformation and digital delivery of government services depends on the extent to which the Australian people can trust and feel secure operating online.

Threats

With the vast opportunity of the internet comes risk. We are not immune from threats to our systems posed by cyber criminals and state-sponsored actors. As people and systems become increasingly interconnected, the quantity and value of information held online has increased and so have efforts to steal and exploit that information.

Australian and overseas organisations across both the public and private sectors have been compromised by either criminal or state-sponsored intrusions. A substantial amount of sensitive commercial and personal information has been lost and significant harm and damage has been incurred to businesses as well as reputations. Figures vary, but cybercrime is estimated to cost Australians over $1 billion each year and by some estimates the real impact of cybercrime to Australia could be around $17 billion annually.

The Australian Cyber Security Centre's *Threat Report 2016* reveals Australian Government networks are regularly targeted by the full breadth of cyber adversaries, from foreign states through to criminals and issue-motivated hacktivists. Foreign states represent the greatest level of threat, but cybercriminals pose a threat to government-held information and provision of services through both targeted and inadvertent compromises of government networks with ransomware.

The Australian Government's ICT systems, particularly the public-facing systems that deliver services to the Australian people, are as much a part of the digital jungle as the systems of

any other government agency or private company. Many of the observations included in this submission are drawn from our experience of the events surrounding the Australian Bureau of Statistics's 2016 eCensus. There are lessons learnt from that event that are relevant to all Australian Government systems owners who delivery digital services to the public.

Key Lessons from the Events surrounding the 2016 eCensus

The events surrounding the 2016 eCensus showed the Australian Government and the public that cyber security is no longer the sole preserve of national security policy-making. Cyber security now includes ensuring the availability of services and confidence in government in a digital age. It showed that confidence, and the trust this confidence provides, are key to successful delivery of digital services. Equally, it showed that system resilience fundamentally underpins the ability to provide trusted, reliable and secure digital services.

The Distributed Denial of Service (DDoS) attacks suffered by the ABS on the first day of the census period were predictable for such a well-publicised event. Furthermore, the Australian public has real and legitimate concerns about privacy and the security of their personal information being collected by the ABS, as the public would for their personal information collected by the any other government agency.

Without reflecting on any particular service offered to the public by government agencies, the ABS is likely not alone. All agencies need to transform their thinking to support truly digital engagement with Australians. And cyber security and privacy were shown to be critical to the confidence of Australians in the online services delivered by government.

Existing systems - Privacy, security, quality and reliability

Successful delivery of digital services to the public relies on government's ability to keep the public's data secure, ensuring privacy. But this will only go part of the way to building the public's trust and willingness to engage with government online. Systems also need to be reliable and deliver a quality user experience in line with public expectation.

Our existing systems, particularly our legacy systems, continue to prove problematic in relation to security and overall resilience. Owners of these systems must be alert to the need to update software and hardware, and understand the limitations of those systems until they can be replaced. I understand that plans are in place to upgrade many systems including moves to centralised capability where appropriate.

Whole of Government digital transformation and digital project delivery

Government agencies' should emulate the best practice of successful e-commerce sites in the private sector by utilising off-the-shelf, scalable analytics software. There are many vendors that offer sophisticated pattern detecting software that can help prevent fraud, identity theft and provide a better experience for the user.

As Government services move online there is a new imperative to embrace cyber security as a core objective for digital transformation. No system connected to the Internet can have guaranteed security. But as more government services move online, project managers will need to address security and respond to security incidents as critical business risks. By making cyber security a core part of system design we will strengthen trust online and build Australia's digital potential.

Security needs to be embedded in all levels of the system architecture, in software and apps as well as applied to the end-points that the public use to access these systems. If we can achieve security within the underlying network layer these systems rely on for their communications so much the better.

Digital literacy, culture

Digital literacy and security awareness, including security risks and consequences, needs to be a core part of agencies' toolkits to deliver services in a modern online economy. Not all agencies, especially smaller ones, are equipped to deliver technology outcomes at scale. Agencies will need to consider alternate service options, such as cloud service provision. Cloud computing can offer significant security, cost and efficiency benefits.

There are opportunities to adopt learnings from the eCensus incident in Phase Two of the government's Digital Transformation Agenda. A key lesson is that security must be 'baked in' to design and delivery. Government can develop more of a 'shared service' consultancy approach to cyber security to boost agency capacity and allow resources to be reallocated to service delivery.

There are also issues arising with the security culture in Commonwealth agencies. There is a prevailing tick box compliance culture. That is, agencies will consider themselves secure if they get their internal ICT area and their subcontractors to put in place and uncritically follow prescribed security procedures. But compliance does not equal security. It is more important that agencies have a culture of security; that they adapt to changing threats and educate their staff on good cyber hygiene. The objective should be to have security culture permeate through agencies, so that they habitually test their systems and arrangements and complacency does not set in. Such an approach will significantly reduce risks to our systems. Noting that we can never eliminate them.

Commonwealth agencies also need to think critically about how they manage their relationships with their vendors. Out-sourcing of technical capabilities is the norm for the Commonwealth and brings challenges to how we manage cyber security risks. Many agencies have long-standing relationships with their vendors, which can lead to complacency in risk management. Trust is good, but trust without verification is dangerous. Contracts can cover the Commonwealth in the event of unavailability of services and lost reputation but they do not do enough to prevent potential damage. Agencies need to verify the security capabilities of their vendors through regular testing and exercises. Agencies should also be cognisant that their ICT contractors also have downstream sub-contractors involved in the service delivery who need to be both trusted and verified.

Another critical lesson learnt from the eCensus event was how we in Government engage with the public in an event or crisis. Social media engagement goes hand in hand with digital transformation. Agencies need to communicate actively with the public when they seek information and reassurance. Clear, simple messaging from the Government through its social media channels can permeate quickly when the public is hungry for useful and meaningful information. This is of critical importance in crisis management, but also has a key role in building trust with public over time as part of business as usual. Agencies that do their business online with the public online need to speak to the public online too. Social media skills need to be raised across the Commonwealth.

Related cyber security issues

Security of personal and financial information is not solely the government's responsibility. The government can only protect what it possesses. Members of the public and businesses dealing with government information should also be aware that their personal information, including but not limited to taxation information, is in their own possession and potentially vulnerable.

Everyone must take responsibility for their online security. Partnering with business and the community to work together to raise the awareness of all Australians to online opportunities and risks is an important element of the Government's Cyber Security Strategy. Fortunately, there are simple steps that any individual or business can take to protect themselves. This includes creating strong passwords, regularly updating software to repair vulnerabilities, being wary of unsolicited emails and avoiding malware by keeping to trusted websites.

Individuals and small and medium businesses are of particular importance in cyber security. The Australian Government has published a Stay Smart Online Small Business Guide and Stay Smart Online My Guide for individuals. These guides provide advice on vital areas of online security including: privacy, passwords, suspicious messaging, browsing safely, online finances and payments, tablets and mobiles, security software and reporting and can be downloaded from the Stay Smart Online website.

Email scams purporting to be from government agencies arise regularly. Warnings to the public about those scams are published by the relevant agencies, the Australian Consumer and Competition Commission's ScamWatch program and by Stay Smart Online on their websites, social media channels and and through their alerts subscription service.

For SMEs, cyber security should be a part of every business's risk management and resilience structures and planning. This includes developing and implementing business continuity, response and remediation plans in the event of cyber security incident. For individuals and business, the cost of implementing measures to protect themselves may be time consuming or in some cases very costly.