servicenow

Cyber, Digital and Technology Policy Division
Department of Home Affairs
Canberra, ACT
techpolicy@homeaffairs.gov.au

24 August 2021

Re : Strengthening Australia's Cyber Security Regulations and Incentives

ServiceNow welcomes the opportunity to contribute towards the governments thinking around strengthening Australia's Cyber Security.

Based on our experience and expertise, this response is focused on Chapter 4 of the Discussion Paper around governance standards. We believe there is an opportunity to use basic governance processes to improve the understanding and awareness of the cyber risks faced by organisations of all sizes.

As an organisation we are committed to supporting government and industry to manage security risks in their digital transformation journeys. We appreciate the opportunity to provide comments and look forward to future opportunities to continue the discussion.

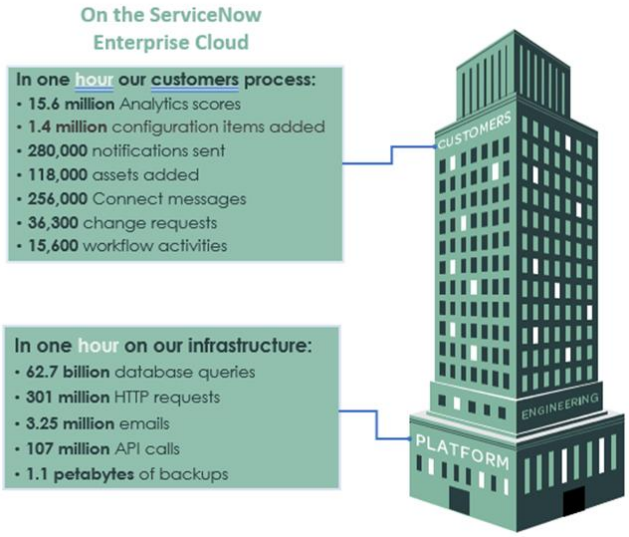
Please feel free to contact me for further information. We would be happy to help inform this critical public policy debate and share our learnings.

John Asquith
Innovation Lead, Government and Higher Education
servicenow.com
[redacted]

servicenow | *making the world of work, work better for people*

About ServiceNow

ServiceNow is an enterprise cloud platform used by most large businesses and government entities in Australia. We are the world's market leader as the system of record for technology assets, and our service catalogue is typically used as the foundation for enterprise service management. We also support these organizations with digital workflows to get things done, often referred to as the 'system of action' in an organization. And with our integrated risk management as a core capability in the platform, and AI driven decision support in real time, we enable a level of responsiveness and resilience that would not have been available in the past. The ability to provide visibility of operations, identify vulnerabilities and respond to issues makes ServiceNow the platform of platforms for enterprise governance.



Helping Australia Address the Problem

"Malicious actors target businesses and individuals who have not implemented basic cyber security measures (regardless of size of the business or the value of data held), and are constantly scanning network services to build a list of future potential vulnerabilities"

Most Australian banks, energy companies, telcos and State/Federal Government entities have chosen ServiceNow to help manage their ICT environments. These organizations are generally very aware of the vulnerabilities they can be exposed to if they have systems that are both connected to the internet and not at the most current patching levels to protect from known threats. They have therefore chosen ServiceNow to help them prioritise and automate the work needed to keep the most vulnerable software up to date.

The ServiceNow platform makes this task significantly easier with

a) AI technologies to catalogue the critical software and hardware components and map these to business services
b) ServiceNow's configuration management database (CMDB) to compare system patch levels with industry threat data, then apply a risk approach to prioritise remediation
c) Our security incident response capability to quickly identify the security issues, protect from further harm, and restore systems as quickly as possible.

However, many large businesses, and most smaller businesses, will currently have neither the awareness nor the capability to minimize their vulnerability to cyber threats in this way.

ServiceNow's Recommendations

Our main area of concern and expertise relates to the contents of chapter 4 in the document which focuses on Governance Standards for Large Businesses.

Many large businesses, especially outside of the critical infrastructure sectors, don't currently have the benefit of such an AI Powered service operations approach, and this leaves them with significant blind spots in their business that can become easy targets for malicious actors.

The most immediate and minimum that can and should be done by any organization is to ensure all employees are aware of the types of threats and how to avoid them. The Essential Eight is a good place to start as this provides a framework for all the measures an organisation can take to protect itself.

However, the threat environment is not going to become any less challenging and the speed at which threats are becoming operationalized is getting faster all the time. It is not appropriate to place the entire security of a business in the hands of its employees, trusting that they will never make a mistake or even willfully harm the organisation. Businesses therefore need to ensure they have

a) visibility of the areas that may be vulnerable to an attack
b) a process for prioritizing and performing the work needed to minimize these vulnerabilities in an efficient and timely manner
c) a governance framework that ensures there are individuals in an organisation who are responsible and accountable for the resources and systems that will minimize their exposure to cyber security threats.

As a minimum, it is critical for any organisation, however small, to maintain a list of its software assets and versions, and to regularly check and update software to ensure currency. This is a discipline that any organization and its management need to consider as an essential part of business, which should be no different from keeping an accurate and current set of financial accounts.

Our recommendation to The Department of Home Affairs on how Government can mitigate some of these risks by developing a strategy for cyber security regulation and incentives are as follows :

Recommendation 1 : *Ensure that all organisations, however large or small, are made aware of and educated around a cyber framework such as the Essential Eight to provide a set of guidelines that can be adopted and followed to minimize their risks. Larger organizations should be required to be able to provide evidence that they have appropriate controls in place to manage these risks.*

Recommendation 2 : *Government should find ways of encouraging, (and if necessary, mandating) large organizations to keep accurate and up to date records of the ICT related software and hardware assets, along with version and patch levels, that are used to operate their business, particularly if connected to the internet.*

Recommendation 3 : *That all businesses should have a nominated contact who is responsible for the 'safety' of the business with respect to security – if you like a 'Fire Warden' for cyber. The responsibilities and accountabilities of the role would depend on the size of the business but should include activities to support implementation of frameworks such as the Essential Eight and assessing and remediating vulnerabilities as thy appear. For large businesses this should require the employment of a Chief Information Security Officer who would drive the governance processes.*