Response to the *Strengthening Australia's cyber security regulations and incentives* discussion paper

(August 2021)

Tanium welcomes the opportunity to provide a response to the Australian Government's *Strengthening Australia's cyber security regulations and incentives* discussion paper.

In Australia, and across the world, Tanium professionals have heard cyber security strategies that talk of a commitment to protecting critical resources, strengthening standards, and improving end user education. This multi-prong strategy is encouraging; but in practice the basics of cyber hygiene are forgotten or neglected by far too many organisations.

Complicating the necessary focus on the basics is cyber security messaging, which largely hinges on the regular update of operating systems and applications, activating multi-factor identification, employee training, antivirus software deployment and law enforcement.

All of these messages are important. However, the need for governments, businesses and individuals to gain and maintain visibility and control of their network endpoints — the top target for cyber attackers — is vital.

The endpoint is the entry to post-compromise activity, and the place where threats and users collide. It must sit at the heart of any cyber security strategy, and with effective solutions available in the marketplace, there is little reason to avoid reckoning with our cyber hygiene — or lack thereof.

You can't protect what you can't see — basic visibility continues to be an issue across the globe

In 2019, nearly all (94 percent) global CIOs that Tanium surveyed admitted to regularly discovering endpoints within their organisation of which they were previously unaware and 70 percent reported doing so on a daily or weekly basis. Over half of these executives (55 percent) said these IT blind spots — perpetuated by tool sprawl, siloed teams, legacy kit and more — could leave them more exposed to cyber-attacks.

Unfortunately, not much has changed in two years, except the advancement of a global pandemic and increasingly distributed workforces to further complicate matters. Gaining visibility is even more challenging in today's IT environments, comprised of on-premises servers and computers as well as work from home endpoints, virtual machines, containers and cloud infrastructure. However, challenges aside, this enterprise visibility must be gained.

Best practice standards and regulations — equipping and empowering organisations

It was heartening to see the Australian Government commit last year to improving baseline security among organisations by enforcing best practice standards and regulations. The move acknowledges the need for consistency and accountability, and the benefits of proactive cybersecurity approaches. A comprehensive strategy for asset and patch management here will also help to drive cyber-resilience by reinforcing IT hygiene. Just throwing money at compliance will not achieve the required results unless the investment is focused on the right areas — the basics.

Of course, solutions to complex problems are not all about surmounting technology challenges. They also involve people who need to be taken on the journey. Cyber-criminals increasingly target their efforts toward the perceived weakest link in the corporate security chain, via the employee endpoint. This reality makes the government's commitment to enhancing cybersecurity awareness among end users and the public-at-large, particularly important.

Understandably, many businesses have been in reactive mode since COVID-19 struck in early 2020. Yet despite 90 percent of surveyed organisations to which Tanium spoke in 2020 declaring their attack frequency had increased, many of the same organisations and more (a full 93 percent) delayed or cancelled key security initiatives. A quarter of those polled (26 percent) said vulnerability management had been bumped down the IT priority list in the rush to support remote working.

It's now time to collectively own cyber security best practices by refocusing on the things that matter. We must start by equipping organisations with knowledge and resources for developing security strategies that include the attainment of clear visibility and control of all digital assets.

The Australian Government has taken a great step in recognising cybersecurity as the foundation upon which to build a prosperous digital society. We're eager to see more detail, including a clear focus on endpoint inventory and management integrated into any new education, guidelines and/or standards. As the government embarks on legislative changes around cyber breach obligations for businesses, and plans for 'secure hubs' for the public service and education of the nation, endpoint visibility and protection must be at the forefront of any strategic plan.

Governance standards for large businesses

The failures of industry transformation to meet the needs of our increasing digital landscape are being uncovered. Everyday Australians are growing more aware of the threats posed to critical infrastructure – and the shared effects that can result.

As the current Critical Infrastructure Bill shows, the protection and service of our public and private frameworks is one of our highest national priorities.

As industries and organisations move to understand their risks and responsibilities, executives and boards must take note and work to better comprehend their compliance requirements. As part of this, cyber security is no longer a matter solely for tech teams—boards must be aware of their organisation's cyber risk and mitigation efforts.

Additionally, we must also be mindful of the costs that compliance will introduce. If the cost of meeting compliance is higher than the penalty or impact of not complying, then we run the risk that the business will accept the risk and either not or partially implement the standard. As we have seen with the implementation of the Essential 8, the ability of agencies to delay implementation due to complexity and obtain exemptions has impacted on the effectiveness of the program.

With the Critical Infrastructure Bill, it's been made clear that the government can direct entities to comply, and it can intervene to provide oversight and demand action. As part of this mandate, strong direction should be included that organisations evaluate their basic hygiene so they can be certain of the protections they have in place, while assuring the government and the Australian people of their safety.

Continued engagement
We welcome the opportunity for further engagement and applaud the Australian Government for actively consulting across industries and with experts to truly develop stronger cyber security regulations and incentives that support a growing digital economy and respond to a growing threat environment.

Contact: Jeremy Roach
Federal Business Lead - Australia and New Zealand
[redacted] | [redacted]