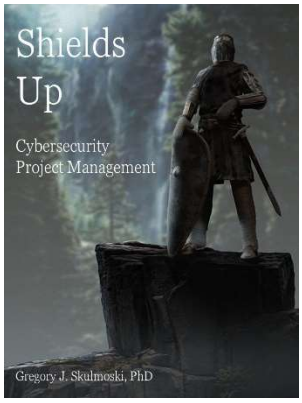
Hello 1 March 2023

Thank you for the opportunity to comment on the *2023-2030 Australian Cyber Security Strategy Discussion Paper.*



I am responding from a project management perspective where I have 15 years of international project delivery experience and almost 20 years in academia. My project management experience is recent where my last project (Smartphone-Connected Pacemaker Devices) won a major innovation award in 2021.

I currently teach project management at the bachelor, master, and PhD levels at Bond University in Australia. I wrote *Shields Up: Cybersecurity Project Management* (2022) and I have completed *Cybersecurity Training: A Pathway to Readiness* (in press, 2023). I am writing *Quantum Cybersecurity; A Transition Plan*. Therefore, I have both practical and academic perspectives on cybersecurity for your consideration.

I have opinions on some of your questions as they relate to my research and practice:

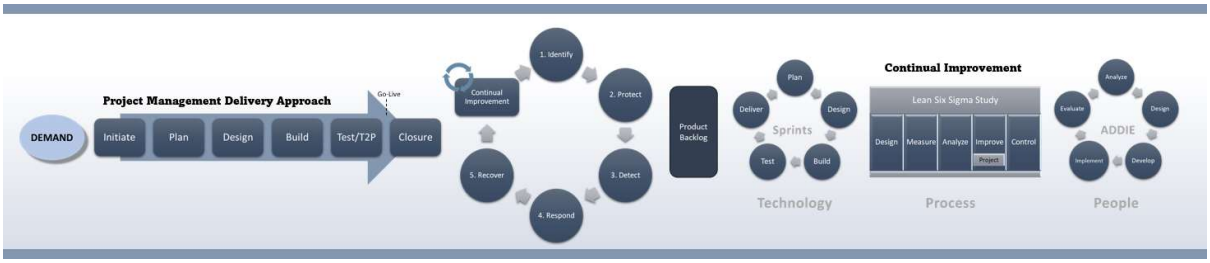
#5 How should Australia better contribute to international standards-setting processes in relation to cyber security, and shape laws, norms and standards that uphold responsible state behaviour in cyber space?

- Standards involvement is critical and the best advice I have is to stay involved with international standards review and development (e.g., the NIST CSF v2.0 is currently under review with an invitation to broad participation. I attended a midnight to 8 am workshop in February.)
- Organizations form “communities of practice” like the Bond University Gaming Community of Practice (to conduct research into simulations and other techniques for the classroom and corporate settings). Communities of practice bring together like-minded people to study to learn about topics of interest. Cybersecurity communities of practice could be supported and encouraged.

#6. How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?

- Align to best practices found in standards and frameworks (e.g., NIST CSF v1.1, ISO 27001, etc.). Be a role model and implement a minimum viable install (e.g., like the Essential 8 controls). However, the Essential 8 are more technical and do not address people or process. Guide businesses and others to implement the Essential 8 and minimum viable installs for ITIL/COBIT and NIST/ISO 27001.
- Follow a maturity pathway that is assessed and reported regularly.
- Since cybersecurity is a digital matter, adopt and excel in either ITIL or COBIT technology service management; one cannot have a robust cybersecurity ecosystem if the foundation (e.g., ITIL) is weak.
- Finally, report your compliance to the standards, but focus on the improved KPIs that standard alignment can bring. Compliance for compliance’s sake often results in uneven quality and residual risk.

- I address your question in my book *Shields Up* and show how organizations can plan, implement, and optimize cybersecurity.



#11. Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?

- While we need more cybersecurity talent (technical through to non-technical roles), the responsibility for cybersecurity has extended beyond our techies; all people are responsible for cybersecurity.
- We need to increase the flow of STEM graduates into our ecosystem, but we also need to provide cybersecurity training to all people on a regular basis, in multiple formats.

#12. What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?

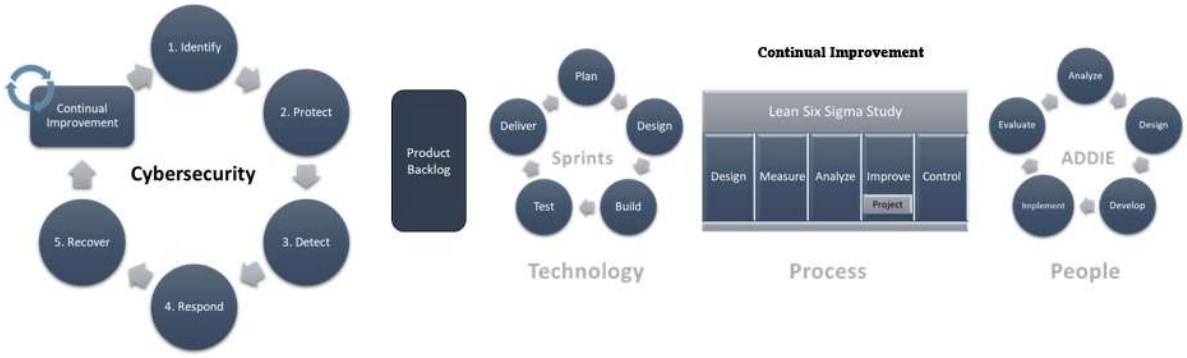
- Encourage universities and other higher education institutions to include cybersecurity awareness training as a core subject.
- Provide incentives for successful skills attainment (e.g., tax reduction).
- Forward looking organizations are taking a holistic approach to cybersecurity where i) cybersecurity is everyone's responsibility and not just IT, and ii) marketing safety, security and privacy as market differentiators. Therefore, I recommend that the *2023-2030 Australian Cyber Security Strategy Discussion Paper* team expand their scope for cybersecurity training and education beyond the technical subject matter experts and upskill all of us and our supply chain partners in cybersecurity hygiene.
- Broaden the support for non-technical cybersecurity roles like project management, training, auditing, legal, etc. who supplement our technical teams. For example, when there is a cybersecurity incident Cybersecurity Incident Response Teams (CSIRT) leap into action to "respond and recover." Ten years ago, our CSIRT included not only technical team members, but also supply chain, finance, and legal team members to work the phones and to document our response and recovery. These non-technical team members freed up our technical team to complete more technical actions as outlined in our Cybersecurity Incident Playbook.
- Support resilience (respond and recover from a cyber incident) improvement efforts such a Resilience Weekends where free workshops are offered to small and medium businesses, community groups, and others. Provide highly-technical resilience workshops for the technical cybersecurity professionals.

16. What opportunities are available for government to enhance Australia's cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?

- I interpret the cybersecurity ecosystem as technologies, people, and processes; each can be delivered and optimized. All three need to be aligned and balanced; we balance cybersecurity with getting on and doing what we need to do.
- Align to existing cybersecurity standards and frameworks built upon either ITIL or COBIT.
- Cybersecurity awareness and training for all people will improve our capabilities to prevent, respond, and recover from cybersecurity incidents.
- Encourage Australian businesses and governments to start planning their quantum transition plan.
- The ONLY way to deliver and enhance the cybersecurity ecosystem is through projects; we cannot buy cybersecurity online or at the store. Therefore, the challenge is to deliver cybersecurity projects in a lean manner that align with international standards. *Shields Up* shows the reader how to achieve their cybersecurity goals with existing standards and frameworks; no need to develop something new.

17. How should we approach future proofing for cyber security technologies out to 2030?

- We cannot future-proof technologies; instead, we optimize until we no longer can extract value (ITIL). We can prioritize the demand for cybersecurity and other technologies, processes, and people optimization, then deliver value incrementally through projects. The ONLY way cybersecurity is delivered and optimized is through projects.



19. How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?

- Both ITIL and COBIT provide a process and framework to address emerging technologies and promote security by design in new technologies.
- Finally, hire practitioners who have experience; you need both policy experts and cybersecurity practitioners who have been bruised. As an academic and practitioner, I read tier-1 research often produced by academics without practical experience. While the theoretical models are appealing, there is poor adoption by practitioners because it does not "fit" into their real world shaped by standards and frameworks. Therefore, balance your team so you can produce implementable solutions.
- We also design-in standards and frameworks

Thank you for this opportunity to contribute and for your fine work.

Sincerely,

[redacted]

Greg Skulmoski PhD, MBA, BEd, CITP, FBCS
Associate Professor, Project Management
Faculty of Society and Design[redacted]
Bond University | Gold Coast, Queensland, 4229, Australia
[redacted]

Books in Print: *Shields Up: Cybersecurity Project Management*
Forthcoming Book: *Cybersecurity Training: A Pathway to Readiness*

https://www.linkedin.com/in/gregoryskulmoski/