Joint Cybersecurity CoP and TAC Workshop – Wed 7th October 2020

Please note *– the focus of this combined workshop will be for each institution's Cyber CoP and TAC members to jointly deliver a presentation (see below for detail), so please start early as each institution will be presenting!*

Intended schedule:
Wed 7th Oct.
9:30am - 12pm: *ACU, Bond, CQU, GU, JCU*
12pm -1:30pm *Break*
130pm -4pm: *QUT, SCU, UQ, USC and USQ*

2020 Cyber Security and Networking CoP Session

Agenda - Joint Presentations
Each institution to have representation from both the Cyber Security Team and Network Team to deliver a joint network and cyber security presentation to cover three broad areas:

1. **State of Play**
    a. Network focus – IT Department team structure, physical and logical network topology, key security controls implemented, describe the core security focus of network team and management of controls.
    b. Cyber Security – Team structure, cover cyber security program and approach, what is the focus in the team for network security.

2. **Challenges**
    a. How do the strategic goals of the institution relate to the work in terms of an overarching vision needed to support activities?
    b. From a networking perspective, what are the current challenges when it comes to current or future network security, for example non-traditional partners etc, asset refresh rates etc
    c. From a cyber security perspective, same as above.

3. **Solutions and Opportunities**
    a. How can these challenges be better met, what solutions can help?
    b. What are the current initiatives or goals in play, current and pending?
    c. What does the future look like? What is an intersectional view?
    d. Along with the challenges, what initiatives or improvements in operation/collaboration could be further developed or achieved from here?

Workshop Purpose, Objectives and Outcomes

1. **Purpose** – to further connect Cyber Security and Network CoP members together with the aim of improving common understanding, communication, relationships and working knowledge of each other's disciplines.

2. **Objectives**
    a. Develop a greater understanding of the approaches and operations of the disciplines of networking and security.
    b. Develop better understanding of intersectional common goals, challenges, solutions, and opportunities.

c. Gain insight into where both security and networking are headed and how future intersections might look and work.

3. **Desired Outcome**
    a. Practitioners will have improved knowledge and understanding of their own institution's as well as other institutions in the two disciplines of cyber security and networking.
    b. A common understanding will assist in improved communication, working relationships and outcomes.
    c. This can be used to facilitate and realise a more effective and adaptive network based cyber security posture.

Look forward to getting together in October to present and share our combined information, it should be a great learning outcome for all!