Paralympics Australia – Cyber Resilience Challenges in National Sporting Organisations for consideration in Horizon 2 of the Cyber Security Strategy

Introduction

Paralympics Australia, as both a peak body for Para Sport in Australia and a National Sporting Organisation (NSOs), plays a critical role in supporting its members athletes, coaches, and clubs nationwide while safeguarding the integrity of elite competition and the broader Paralympics community. Increasing digitisation of sporting administration, athlete performance monitoring, and fan engagement has brought significant benefits. However, this reliance on digital platforms has introduced new vulnerabilities that threaten the security, continuity, and reputation of the sport.

Paralympics Australia partners with Government, Members, National Sporting Organistions (NSOs) and State Sporting Organisations (SSOs) as well as a range of sports clubs and schools at the local level. Across this eco system of partners each partner is an independent business and has independent governance obligations. At the local clubs and schools' level most of these local clubs are volunteer-led organisations constrained by limited budgets. Information and data is shared across and between all levels of the Paralympics Community which is working to achieve digitisation across the Paralympics eco-system.

This response outlines the specific cyber resilience challenges faced by Paralympics Australia and the broader Para Sport sector, including many small-to-medium sporting bodies in Australia. It is submitted for consideration under Horizon 2 of the Cyber Security Strategy.

Resource Constraints

Unlike larger government agencies or corporations, Paralympics Australia operates within limited financial and staffing resources. Whist supported by Government Paralympics Australia relies on commercial partners and the generosity of donors to support its operations. Cyber security often competes with immediate operational priorities, such as athlete development programs, international and domestic competition costs, classification and athlete pathways as well as participation funding and general business oeprations. These competing priorities create challenges in maintaining up-to-date cyber defences, continuous monitoring, and access to skilled cyber professionals.

Sensitive Data

Due to the nature of Paralympics Australia, the organisation manages important information to support its people and operations including athlete data, member records, donor information and commercial arrangements. Protecting this information is critical to maintaining privacy, safeguarding organisational integrity, and upholding trust with our stakeholders and partners. Any unauthorised access or loss of this information could undermine these commitments.

Increasing Threat Environment

Sporting organisations are increasingly attractive targets for cyber adversaries:

- **State actors** may target elite sporting bodies to obtain sensitive training data or disrupt operations around international events.
- **Criminal groups** exploit vulnerabilities for financial gain, such as ransomware attacks or payment fraud.

Paralympics Australia, while not a high-profile financial target, is vulnerable to opportunistic attacks that exploit weaker cyber maturity compared to larger sectors.

Supply Chain and Technology Dependencies

Paralympics Australia depends on external vendors for cloud-based member management systems, athlete performance analytics, and communication platforms. These third-party systems can be both enablers and risks, as supply chain vulnerabilities may be outside the organisation's direct control but still impact operations. Additionally, Paralympics Australia relies on digital timing, video review, and event management systems that, if compromised, could disrupt major competitions.

Limited Access to Sector-Specific Guidance

Cyber security frameworks such as the Essential Eight and the Protective Security Policy Framework (PSPF) provide strong baselines but are not always readily translatable to the operational context of the sports sector. Paralympics Australia, like many sporting bodies, would benefit from tailored, practical, and cost-effective guidance that considers its unique environment and constraints.

Building a Cyber Aware Culture

Athletes, coaches, administrators, and volunteers all interact with digital systems, often on personal devices with varying levels of cyber awareness. Creating a culture of cyber vigilance across such a diverse and decentralised user base is a significant challenge. Awareness training must be accessible, sport-specific, and reinforce good cyber hygiene practices at all levels of the Paralympics community.

Opportunities for Horizon 2

Paralympics Australia supports the ambition of the Australian Cyber Security Strategy to extend protections and uplift cyber resilience across all sectors. Horizon 2 presents an opportunity to:

1. **Develop a Sporting Sector Cyber Resilience Program** – tailored support, guidance, and information sharing for NSOs and the Para Sport sector.
2. **Enable Access to Affordable Shared Services** – such as managed SOC, penetration testing, and cyber insurance designed for small-to-medium sporting organisations.

Conclusion

Paralympics Australia recognises the critical importance of strengthening cyber resilience to protect its athletes, data, and reputation. However, the resource and capability constraints common to NSOs present real challenges in implementing mature cyber defences. Horizon 2 of the Australian Cyber Security Strategy provides a vital opportunity to address these sector-specific needs, ensuring that sport in Australia, as an essential part of national identity and community wellbeing, is protected from evolving cyber threats.

Paralympics Australia