Cyber Security and Risk Management

Protecting your Data & Devices while Navigating the Human Element

TRAINING

Network and Data Security through Technology and Training your Workforce

Facilitated by
PHILIP WAGNER
Director of Cyber Security
NDIA

Online → **16 & 23 February 2022** | 10am – 2pm AEDT

PUBLIC SECTOR NETWORK

Certified B Corporation

Network and Data Security through Technology and Training your Workforce

Cyber security and the protection of data are a priority across all levels of government. As Australian organisations proactively try to remain ahead of network breaches and threats from bad actors, employing the latest methods of device and data protection has become essential. Implementing the latest technology and protecting endpoint devices is paramount to the protection of public data entrusted to government organisations.

As cyber threats evolve, so do the methods employed to respond and react to them. Implementing tools to counter threats, while informing a reticent workforce, has become one of the biggest challenges to date. Constant system monitoring and consistent communication with personnel to inform them of upgrades, ensures everyone works together to keep information secure.

Through an innovative mix of lecture-style presentations, interactive group exercises and expert feedback, participants will learn the latest methods in network and data protection. They will discover how to communicate the necessity of cyber security to colleagues and how to express cyber risk in a meaningful way. They will find out how to create a strategy for change and the ways in which to translate technical impacts to business impacts for non-cyber people.

This training session provides you with all the tools and techniques to apply best practice cyber security principles. Participants leave with theoretical and practical knowledge, as well as a functional process that can be immediately applied to shape cyber strategy and implement change.

Not Just a Training Session

- Discuss techniques to create a strategy for change and communicate why it is important
- Learn about the latest in cyber security technologies to help make your organisation proactive against threats and bad actors
- Put theory into action by working in groups to prepare presentations to translate technical impacts to business impacts and receive constructive, real-time feedback
- Work on practical cyber strategies that bolster your data and network protection
- Leave with a functional knowledge of how to translate technical impacts of cyber threats to business impacts
- Walk away with a course content pack including slide decks, session recordings and templates

Who Attends

The Protecting your Data and Devices while Navigating the Human Element training session has been specifically designed for anyone that works in the cyber security or risk management space. It is for those looking to expand their technical knowledge, understand how to implement greater protections for their data and networks and learn how to translate the technical impacts to business impacts for non-cyber people.

The course is suitable for any public sector professional with basic knowledge of data and device protection techniques, those looking to refresh their skills and explore new approaches and analysts looking to formalise their training with cyber security best practices.

Meet Your Facilitator

PHILIP WAGNER
Director of Cyber Security
NDIA

Philip Wagner is a leadership educator, trainer, executive coach and project/program manager, with extensive leadership and project management expertise in both civilian and military environments and had key client relationships with Commonwealth agencies including Department of Defence, Bureau of Meteorology and IP Australia.

Currently, Phil is leading the cyber security team in the public sector space at the NDIA.

His achievements to date:

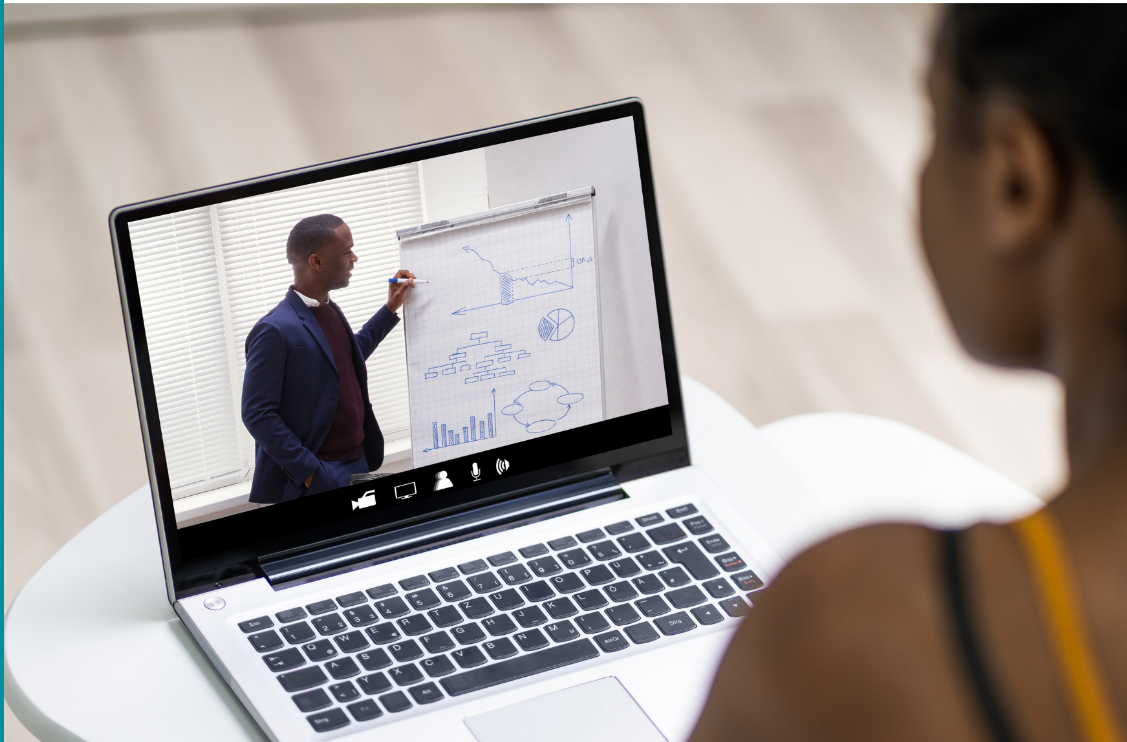
- While working for NAB Technology Projects division, he built one of the most consistently high performing technology development teams at NAB.
- At EDS Australia, his task was to deliver a new payments solution while developing and leading a large new technology team.

Preparation

This workshop is highly interactive with group activities and discussions throughout. Come prepared with some current challenges you are facing in your organisation.

- To participate you'll need:
- A computer with camera and microphone
- Strong internet connection
- Quiet, well-lit space
- Current challenges you are facing

CLICK HERE TO REGISTER



Explore the Agenda

Day 1 - 16 February

Module One – Design and Build Protection Strategies

10:00am	**PSN Welcome and Introductions**
10:05am	**Training Overview, Objectives and Outcomes and Icebreaker** • Introduction • Quick Poll and Q & A
10:20am	**Understanding the current environment** • How did we get here? • What are the biggest threats to your organisation?
11:00am	**Developing Your Organisation's Approach** • Understanding risk • Understanding and implementing cyber first principles: Developing your approach in protecting your data and devices while navigating the human element • The layered defence approach
11:40am	**Breakout Activity:** **Assess Your Organisation's Cyber Strategy Against Best Practice Guidelines Discussion:** 1. What are your top 3 threats? 2. What is your organisation's current approach to risk 3. What are you doing/not doing in the categories: 'Yourself, Your Staff, Your Systems, Your Surroundings, Your Data, Your Crisis Response'?
12:00pm	**Lunch Break**

Module Two – From Policy to Process to Technology

12:30pm	**Conveying the Need for Proactive Cyber Security to Non-Tech People** **Policy and Process** • Achieving a balance - The FASS approach to cyber security – 'Yourself, your staff, your systems, your surroundings, your data, your crisis response' • Policy – process – technology • The FASS Approach: (Feasible, Achievable, Suitable, Sustainable) **Risk** • Identify - what must be protected (non-negotiables) • Identify - what risks are acceptable **Stakeholder Engagement and Communications** • Who needs to be involved; how this will this impact them? • Communicating cyber risk in a meaningful way • Developing a communications /change approach that works **Governance and Oversight** • The role of governance in your protection strategy • Setting up and implementing sound oversight practices **Technology** • Initial identification of technology • Selection and evaluation criteria • Principles of technology selection - Protecting endpoints to keep your network secure
1.30pm	**Breakout Activity:** **Develop Policy (policy & process template & example provided)** **What to write (intent, language)** • Develop a draft Policy Statement • Develop 1 x Processes
1:50pm	**Homework Discussion**
2:00pm	**Close**

Day 2 - 23 February

Module Three – Developing Your Cyber Technical and Communications Approach

10:00am	**Welcome Back and Homework Discussion** **Activity: "Gentle Reminder"**
10:20am	**Technology and Communications (Practical – Q & A)** • From Day 1: • Assess technology selection • Confirm technology selection • Develop communications approach to and with key stakeholders
11:10am	**Group Project Work** • Finalise Policy and Process • Develop Presentation
12:30am	**Lunch Break**
1:00pm	**Group Project:** **Verbal Presentation – to key stakeholders**
1:50pm	**Summary and Closing Notes from Facilitator** **Session Feedback**
2:00pm	**Close**

CONNECTING GOVERNMENT
WWW.PUBLICSECTORNETWORK.CO

AUSTRALIA / NEW ZEALAND
P +61 2 9057 9070
E info@publicsectornetwork.co

USA / CANADA
P +1 (647) 969 4509
E contact@publicsectornetwork.co

PUBLIC
SECTOR
NETWORK

Certified
B
Corporation