



# Cybersecurity Preparedness and Response for Local Government

TRAINING

Defending Local Government's security  
frontline for cyber battle readiness



Facilitated by  
**PHILIP WAGNER**  
Principal Cyber Security Specialist and Educator  
G.P.Wagner Pty.Ltd

Online → 26 & 27 March 2024



## Overview

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.

As cyber threats evolve, we need to understand:

- What these threats mean and represent
- Develop our intent and approach to them
- Develop and implement methods to respond

Local Governments face the additional challenges of:

- Limited IT budgets
- Resourcing constraints
- Compliance requirements resulting from legislation and regulation

Through an innovative mix of lecture-style presentations, interactive group exercises and expert feedback, participants will learn how to develop the most suitable cyber security approach for their local government area.

Participants will learn how to communicate the necessity of cyber security to their local government 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 local government staff.

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.

## Learning Outcomes

- Understand the challenges faced by Local Government
- Develop your cyber security approach using the PPTT(Policy, Process, Technology and Training) approach
- How to use the FASS (Feasible, Achievable, Suitable,Sustainable) formula to assess and determine the most suitable approach for your Local Government area
- Put theory into action by working in groups to prepare presentations to translate technical impacts to business impacts and receive constructive, real-time feedback

## Who Should Attend

The **Cybersecurity Preparedness and Response for Local Government** training session has been specifically designed for:

- IT Managers and Administrators
- Information Security Officers
- Cybersecurity Managers, Analysts or Engineers
- Network Administrators
- Risk Management Managers or Specialists

## Why Attend

- Expand your overall cyber security knowledge
- Understand how to implement greater protections for their data and networks within their Local Government environment
- Learn how to translate the technical impacts to non-cyber people including councilors, local government executives and staff
- How to assess and determine the most suitable approach for your Local Government area

## Meet Your Facilitator



**PHILIP WAGNER**  
Principal Cyber Security Specialist  
and Educator  
G.P.Wagner Pty.Ltd

Philip Wagner is a cyber security, leadership educator, trainer, executive coach and project/program manager, with extensive leadership and project management expertise in both civilian and military environments. He has advised and trained in a wide range of industries from banking and finance, education and training, technology and government at federal and state levels.

His most recent roles were as the Director Cyber Security and Deputy Chief Information Security Officer with the National Disability Insurance Agency and as a Senior Project Manager for a major Australian Health provider in developing their Cyber program.

## 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

## Register Early & Save

Extra Early Bird	Early Bird	Standard Price
Register by 27 <sup>th</sup> Oct	Register by 24 <sup>th</sup> Nov	Register by 25 <sup>th</sup> Mar
\$795 + GST	\$995 + GST	\$1,195 + GST
Save \$400	Save \$200	-

**CLICK HERE TO REGISTER**

\*Group Discounts Available - Contact Registration at [registrations@publicsectornetwork.com](mailto:registrations@publicsectornetwork.com) or Call on **(02) 9057 9070**

# Explore the Agenda

DAY 1 | Tuesday, 26 March 2024, 10:00am - 2:30pm AEDT

---

## 10:00am Welcome and Introductions

### Module 1: Introduction and Challenges for Local Governments in Australia

## 10:15am Understanding the state of cyber security in Local Government

- How did we get here
- What do you believe are the biggest cyber and IT challenges to your Local Government Area
- What is the state of your current cyber measures
- What the State Auditor Generals are saying

### Module 2: Setting up the Foundations

## 11:00am Evaluating the FASS Approach and PPTT Approach

- A Case Study: How a cyber attack affects business and workflow
- Achieving the balance - the FASS Approach to Cyber Security
- The 6 required areas of cyber security
- The PPTT approach: Policy, Process, Technology, Training
- Compliance requirements

## 11:50am Lunch

---

## 12:20pm ACTIVITY: Developing a Cyber Security Policy

- Developing your Local Government Policy Approach
- Developing your processes
- Assessing your Technology
- Develop your Cyber security approaches
- Assess through FASS

## 01:05pm Mapping out Next Steps

- **DISCUSSION:** This session reviews and discusses learnings from Module 2
- What have we learned?
- What are the key actions that need to be taken?
- Next steps: What is the priority of effort

## 01:50am Break

### Module 3: The People Element

## 01:55am Communicating Cyber risk in an Affective Way

- Communicating cyber risk in a meaningful way within Local Government
- Identifying Key Stakeholders
- Creating and building the connections and partnerships required to implement your cyber security approach

## 02:25pm Reflections and Closing remarks

## 02:30pm End of Day 1

---

# Explore the Agenda

DAY 2 | Wednesday, 27 March 2023, 10:00am - 2:00pm AEDT

---

**10:00am** Welcome and Review of Day 1

## Module 4: Communication and Compliance

**10:15am** Communicating the People Element in Cyber for Local Government

- Who are our key stakeholders?
  - What are their information requirements
  - Communication and Messaging: What works best in you LGA
- 

**11:00am** Comfort Break

**11:10am** Compliance and Regulation

- Understanding the cyber compliance and regulation requirements applicable to local government
  - What cyber standards (NIST, ISM, ISO) are most suitable and relevant to your local government area
  - Steps to meet legislative and regulatory compliance
- 

**12:00pm** Lunch

---

**12:30pm** Putting together and Implementing the Cyber Security Jigsaw Puzzle

**ACTIVITY:** This interactive session goes through the steps required to put together your cyber security plan and approach including:

- Review of your Plan from Module 2
  - Governance and Oversight
  - Resourcing
  - To outsource or not to outsource
  - Risks, mitigations and treatments
  - Communication with stakeholders
  - Training of staff
- 

**1:50pm** Closing Remarks

**02:00pm** End of Day 2

---



## Get In Contact

CONNECTING GOVERNMENT  
[PUBLICSECTORNETWORK.COM](http://PUBLICSECTORNETWORK.COM)

### AUSTRALIA / NEW ZEALAND

**P** +61 2 9057 9070

**E** [info@publicsectornetwork.com](mailto:info@publicsectornetwork.com)

### USA / CANADA

**P** +1 (647) 969 4509

**E** [contact@publicsectornetwork.com](mailto:contact@publicsectornetwork.com)

JOIN THE SOCIAL LEARNING PLATFORM FOR FREE AT [PUBLICSECTORNETWORK.COM](http://PUBLICSECTORNETWORK.COM)