



A Roadmap to Ransomware Resilience

TRAINING

Keeping the public sector safe from malicious cyber attacks



Facilitated by
BRENDAN NEWELL
General Manager
CyberPathways

Online → 7 & 14 August 2024



PUBLIC
SECTOR
NETWORK



Overview

With ransomware attacks on the rise, how safe is your organisation?

Australian government departments are increasingly being targeted by cyber-attacks. Attempts to steal government data have increased by over 60% in recent months and this is unlikely to decrease. Malicious acts will continue to increase in reach and sophistication.

The public sector needs to significantly bolster its defensive forces in the fight against ransomware attacks. Significant strides are being made towards this with the \$600 million Cyber Security Strategy announced at the end of 2023.

However, one of the biggest challenges is the knowledge gap and shortage of skills to address such vulnerabilities. If you are beginning your ransomware resilience journey, you have come to the right place. This program has been put together for cyber security specialists with a view to educate, upskill and build actionable insights.

This training will enable participants to explore and gain insights on cybersecurity best practices, improve incident response and preparedness skills, educate others and craft effective backup strategies to build and maintain a ransomware resilient organisation.

Who Should Attend

- IT Support Officer
- Systems Administrator
- Network Administrator
- Cybersecurity Analyst
- Information Security Officer
- IT Security Specialist
- Data Protection Officer
- Helpdesk Technician
- Desktop Support Technician
- Risk Management Officer
- Digital Transformation Officer
- End User Computing Specialist
- Cybersecurity Literacy Trainer
- Application Support Analyst

Learning Outcomes

- Recognise the mechanics of ransomware attacks and their implications
- Identify and mitigate common cybersecurity vulnerabilities
- Implement best practices and strategies to enhance the security and resilience
- Utilise available resources and reporting channels effectively in the event of ransomware incidents

Why Attend

- Benchmark and network with peers from all over the public sector
- Gain a critical cybersecurity skill
- Understand the questions you need to be asking
- Dial-in from anywhere!
- Gain the opportunity to be a part of a community of practice

Meet Your Facilitator



BRENDAN NEWELL
General Manager
CyberPathways

Brendan Newell is an experienced educator and dynamic education and training professional who has been responsible for leading a number of learning teams and development programs spanning several technical domains (electrical engineering, computing, integrated logistics, battlespace management and program management). Brendan has worked in large international companies, building upon a diverse array of work in educational contexts, nationally and internationally in local and federal government and private education institutions. He excels in developing strategic initiatives and applying his project management skills during the execution of such programs. He enjoys working with education and learning professionals and helping them tackle challenging situations by assisting them in developing strategies and skills to help them achieve their desired outcomes.

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

Register Early & Save

Extra Early Bird	Early Bird	Standard Price
Register by 24 th May	Register by 21 st Jun	Register by 6 th Aug
\$795 + GST	\$995 + GST	\$1,195 + GST
Save \$400	Save \$200	-

CLICK HERE TO REGISTER

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

Explore the Agenda

DAY 1 | 7 August 2024, 10:00am - 02:30pm AEST

10:00am Opening Remarks

- Welcome
- Introductions
- Overview and Setting Expectations

Module 1: Introduction to Ransomware

10:30am Understanding Ransomware

- What is Ransomware?
- Common Attack Vectors
- Impact of Ransomware

11:45am Urgency for Public Safety Organisations

- Public safety services and their vulnerability to ransomware
- Potential consequences of ransomware attacks
- Proactive measures and preparedness for mitigating ransomware risks

12:30am Lunch Break

Module 2: Cybersecurity Fundamentals

1:00pm Common Vulnerabilities

- Phishing attacks and social engineering tactics in ransomware
- Exploiting software vulnerabilities and the risks of using outdated systems
- Lack of robust cybersecurity policies and employee awareness as vulnerabilities

1:45pm Securing Networks Against Ransomware

- Implementing multi-layered security measures
- Regular software updates and patch management for vulnerabilities
- Backup and recovery strategies for critical data

2:30pm End of Day 1

Explore the Agenda

DAY 2 | 14 August 2024, 10:00am - 02:30pm AEST

10:00am Welcome and Recap

Module 3: Resilience Strategies

10:15am Prevention Best Practices

- Risk assessments and vulnerability scans
- Training employees on recognizing and reporting phishing attempts and suspicious activities
- Establishing incident response teams and protocols

11:00am Response Best Practices

- Developing and testing incident response plans
- Engaging with cybersecurity experts
- Implementing communication protocols and public relations strategie

12:00am Lunch Break

Module 4: Incident Response and Reporting

12:30pm Incident Response and Reporting

- Identifying and isolating infected systems
- Decrypting data or restoring from secure backups.
- Documenting the incident
- Conducting post-incident analysis
- Reporting Incidents
- Analysing response strategies and effective mitigation

1:00pm Case Studies

- Analysis of past ransomware incidents and lessons learned

2:15pm Closing Remarks

2:30pm End of Training

Feedback from earlier training sessions

“Very relevant for me in my role, informative and well targeted, helpful information and resources.

“It was great. I learned a lot and I feel I got value for money.”



Get In Contact

CONNECTING GOVERNMENT
PUBLICSECTORNETWORK.COM

AUSTRALIA / NEW ZEALAND

P +61 2 9057 9070

E info@publicsectornetwork.com

USA / CANADA

P +1 (647) 969 4509

E contact@publicsectornetwork.com

JOIN THE SOCIAL LEARNING PLATFORM FOR FREE AT PUBLICSECTORNETWORK.COM