CYBER TRAINING ROADMAP

A Guide to Building Your Cybersecurity Skills

Cyber 365

About Us: Chris Ward and Cyber 365

At Cyber 365, we're dedicated to building a resilient cybersecurity landscape, one that helps organisations defend, prepare, and stay ahead in today's rapidly changing digital world. Led by our founder, Chris Ward, Cyber 365 brings expertise, innovation, and practical cybersecurity solutions to businesses, institutions, and government agencies around the globe.

Meet Chris Ward: A Cybersecurity Leader with Global Impact

Chris Ward is more than just a cybersecurity professional; he's a leader with a deep understanding of the challenges facing organisations today. As a seasoned expert and an official partner of the Software Engineering Institute (SEI), Chris holds a unique advantage in delivering SEI-authorised CERT Information Security training. His mission? To empower organisations of all sizes to effectively manage their cybersecurity risks and develop a robust, secure infrastructure.

With extensive experience in both public and private sectors, Chris has led cybersecurity initiatives worldwide. He has guided teams across New Zealand, Australia, the South Pacific, and beyond, helping organisations develop resilient strategies against cyber threats. Chris combines technical expertise with a hands-on approach, ensuring that Cyber 365 delivers practical, accessible cybersecurity solutions that make a difference.

Our Mission at Cyber 365: Simplifying Cybersecurity

At Cyber 365, we believe cybersecurity should be accessible to all organisations, not just those with large IT departments. We know that effective security starts with understanding. Our mission is to simplify cybersecurity, equipping businesses with tools and training that are clear, actionable, and aligned with best practices. From online training to specialised workshops, our services are designed to build cybersecurity resilience at every level.

Cyber 365 Services

Cyber 365 provides a wide range of cybersecurity services, tailored to the unique needs of our clients:

- Training and Workshops: From fundamental cyber awareness to advanced incident handling, our programs help businesses build essential skills and protect their digital assets.
- Consulting and Risk Assessments: We work with organisations to assess vulnerabilities, build effective cybersecurity strategies, and implement customised policies that align with industry standards.
- Cyber Resilience Reviews: We evaluate an organisation's cybersecurity posture, identifying areas of improvement and strengthening resilience against evolving threats.

Why Choose Cyber 365?

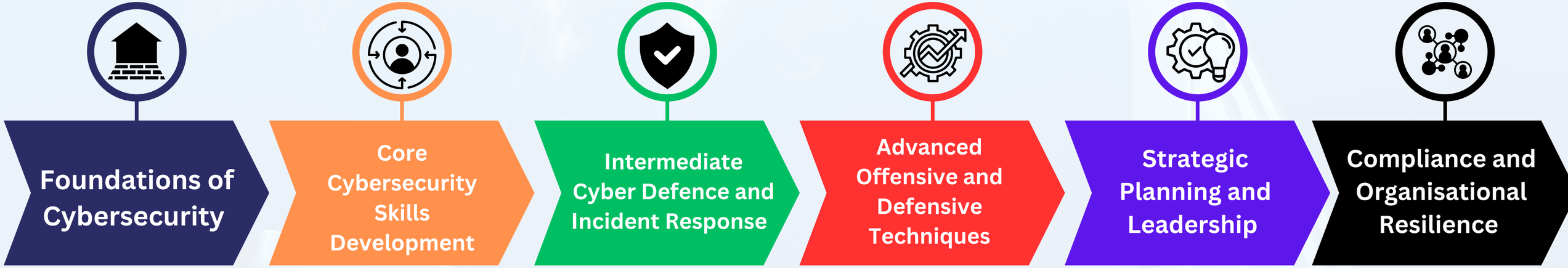
Our approach is both strategic and hands-on. At Cyber 365, we combine advanced knowledge with practical training to provide solutions that are not only effective but also adaptable to real-world applications. We're proud to empower businesses with the confidence to operate securely in a digital world.

With Chris Ward and Cyber 365, you're not just getting a service—you're gaining a partner in cybersecurity. Explore how we can help you strengthen your cyber defences at cyber365.co.

Cyber 365

CYBER TRAINING ROADMAP

A Guide to Building Your Cybersecurity Skills



A strategic guide for developing a cybersecurity-savvy workforce.

Cyber 365

Foundations of Cybersecurity

- Cyber Awareness for All Staff Workshop (1.5 hours): Ideal for all employees, introduces basic cyber hygiene, threat awareness, and individual responsibility in maintaining cybersecurity.
- Fundamentals of Incident Handling (5-day Workshop): For those new to incident response, covers initial response steps, common threats, and incident management essentials.

Cyber Defence and Incident Response

- Deploying and Managing Incident Management Tools (2-day Workshop): Teaches the setup and management of incident response tools, moving from theory to practical applications.
- Advanced Incident Handling (5-day Workshop): Builds on initial incident handling skills with advanced detection, response, and recovery techniques for more complex incidents.
- Penetration Testing and Vulnerability Assessments (3-day Workshop): Focuses on identifying system vulnerabilities through ethical hacking and testing tools, critical for strengthening defences.

Strategic Planning and Leadership

- Creating a Cybersecurity Incident Response Team (CSIRT) (1-day Workshop): Guides the setup of a CSIRT, including team roles, procedures, and tools, preparing organisations to manage incidents in-house.
- Deploying a CSIRT Workshop (5-day Workshop): For those ready to operationalise a CSIRT, covers the implementation of policies, tools, and team coordination.
- Cyber Training Roadmap Workshop (1-day Workshop): Helps organisations design tailored training paths for teams, ensuring consistent skills development in line with organisational needs.
- Cyber Capability Maturity Model (1-day Workshop): Assesses the organisation's cyber maturity level, providing a roadmap for continuous improvement and strategic cyber growth.

NOTE: Some workshops are available as an online course.

Core Cybersecurity Skills Development

- Technical Writing for Incident Handlers (1-day Workshop): Builds effective reporting and documentation skills, essential for incident handlers at all levels.
- Cyber Resilience Review Workshop (3-day Course): Covers essential cyber resilience strategies, such as disaster recovery planning, proactive threat management, and resilience best practices.
- MITRE ATT&CK Threat Framework (1-day Course): Provides insight into mapping adversarial tactics and techniques, useful for understanding attacker behaviors.

Advanced Offensive and Defensive Techniques

- Defensive Cyber Attack Techniques (2-day Workshop): Explores defensive measures, including network monitoring, active threat detection, and real-time response strategies.
- Offensive Cyber Attack Techniques (2-day Workshop): Covers offensive tactics, providing insights into attacker methodologies to better defend against them.
- Attribution Techniques (1-day Workshop): Introduces skills for tracing cyber-attacks to their sources, enhancing investigative capabilities in complex incidents.
- Avoiding Attribution Techniques (1-day Workshop): Examines tactics attackers use to evade detection, helping defenders anticipate and counter evasion strategies.

Compliance and Organisational Resilience

- Understanding the NIST and ISO Frameworks (1-day Workshop): Provides an understanding of key cybersecurity frameworks for organisations aligning with international standards.
- Insider Threat Training (3-day Workshop): Specialised training to identify, mitigate, and manage insider threats, essential for protecting sensitive data.
- Privacy Impact Assessment: Covers privacy compliance and data protection essentials for regulatory adherence.