



# ACADEMIESAUSTRALASIA

THE POSSIBILITIES ARE INFINITE

## The Importance of Education in Cyber Security 教育在網路安全中的重要性

Paul A. Watters PhD 教授主講  
Academic Dean 高等學院院長,  
AAPoly  
<[p.watters@aapoly.edu.au](mailto:p.watters@aapoly.edu.au)>

# Overview

What is  
Cyber  
Security?

Awareness,  
Training,  
Education

People,  
Process,  
Technology

Questions

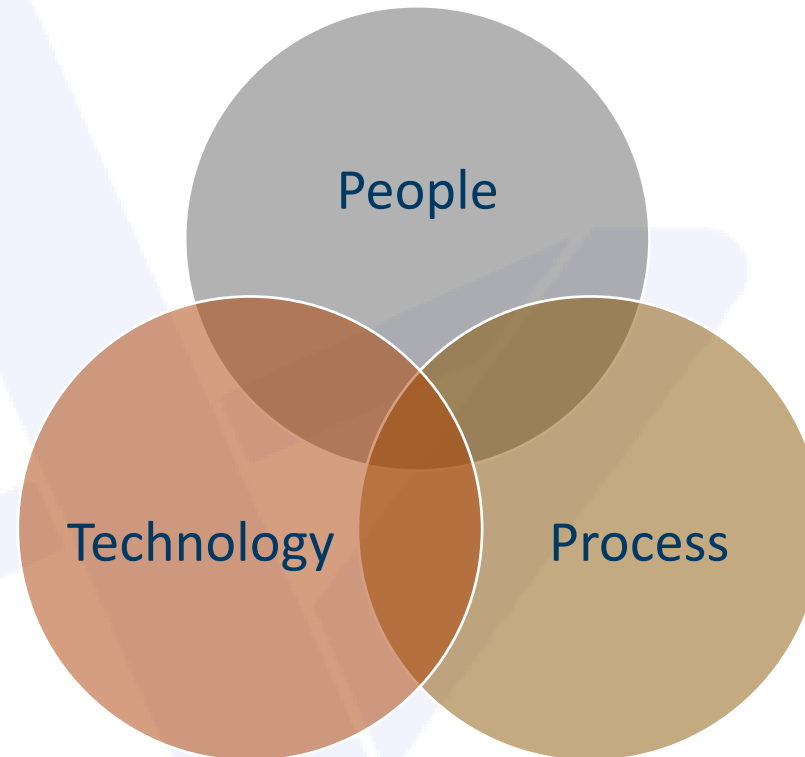
# What is Cyber Security?

## **Any program of work that reduces risk in cyberspace**

- Variety of threat actor motivations
  - Espionage – foreign government / corporations
  - Fraud / extortion – cybercrime gangs and organised crime
- Layers of responsibility
  - Government
  - Business
  - Law enforcement

# What is Cyber Security?

**People – Process – Technology Framework**



# How are cyber attacks performed?

- **Penetration of infrastructure**
  - Unpatched system and network vulnerabilities
  - Use of default passwords
- **Exploitation of flaws in crucial business processes**
  - Lack of governance / oversight /planning
- **Human behaviour attacks**
  - Phishing
  - Scams
  - Insider threat
  - Weak / memorable / guessable passwords

# AAPoly Course Rationale

- Australia's first Bachelor degree to focus on training graduates in GRC
  - Broad education in cognate business disciplines – law, marketing, economics, accounting etc
  - Ability to read, interpret and implement programs according to regulations and standards
  - Core sequence in GRC aligned to international requirements
    - Program Development, Risk Assessment and Mitigation, Forensics, Cyber Law, Ethics, Governance, Incident Response, Analytics

# AAPoly Course Rationale

- Cyber Security is NOT an IT problem
  - It is a BUSINESS problem for which the partial solution may involve IT
  - Key elements: Governance, Risk, Compliance (GRC)
- Governance
  - Design and implementation of a cyber program to reduce risk
- Risk
  - What is likely to be attacked, and how can the risk be mitigated?
- Compliance
  - Will I be fined if I do something wrong?

# AAPoly Course Rationale

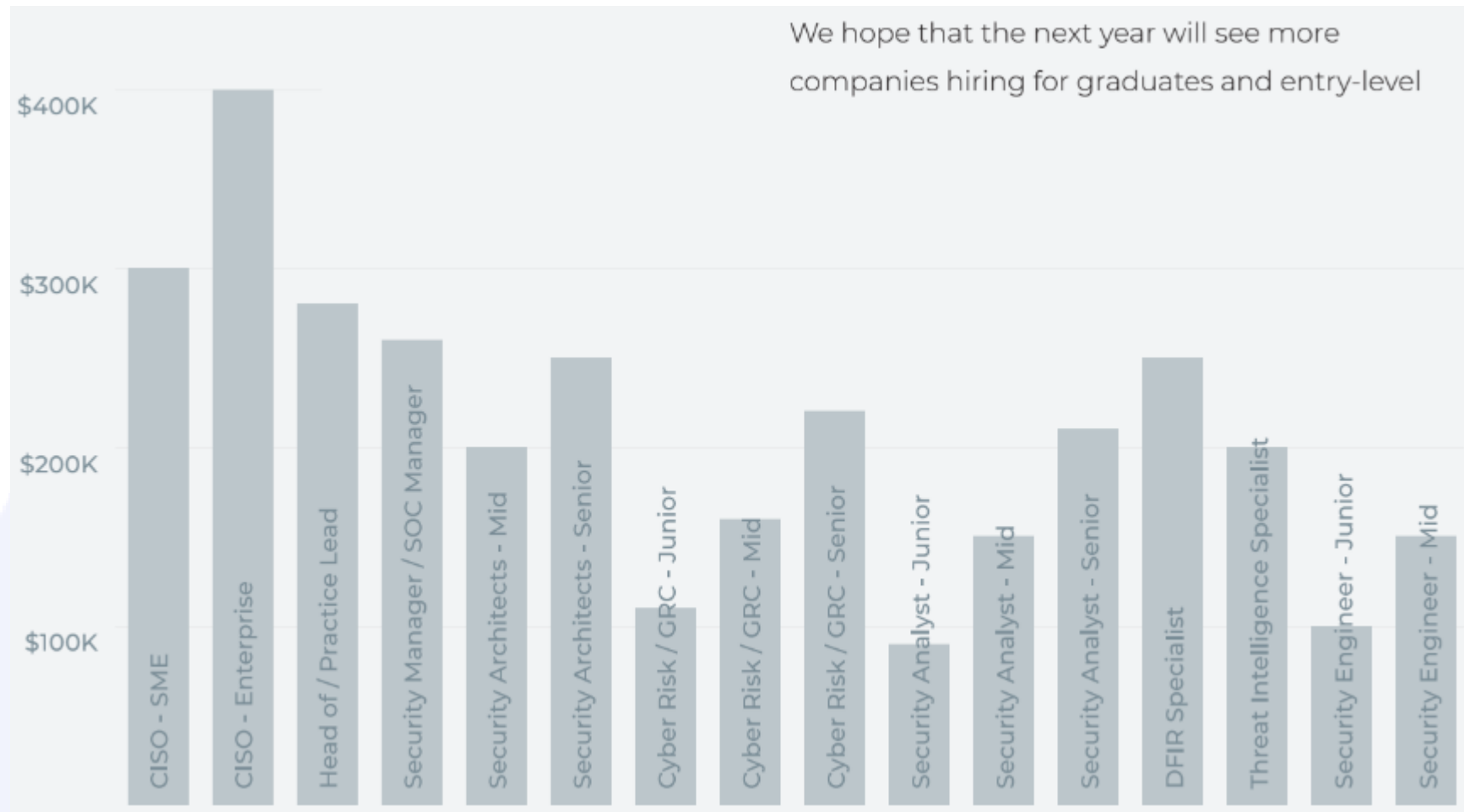




# Labour Imperatives

- AustCyber Sector Competitiveness Plan
  - Severe shortage of job-ready cyber security workers
  - Core cyber workforce has increased 13% to 20,500 workers over past three years
  - Nearly 17,000 more cyber security workers needed by 2026 (just in Australia)
- Taiwan National Cyber Security Program (2021-2024)
  - Expand the quota of cyber security educators and teaching resources in higher education
  - Facilitate the cultivation of cyber security professionals and the quality of teaching

# Average Salaries – Decipher Bureau



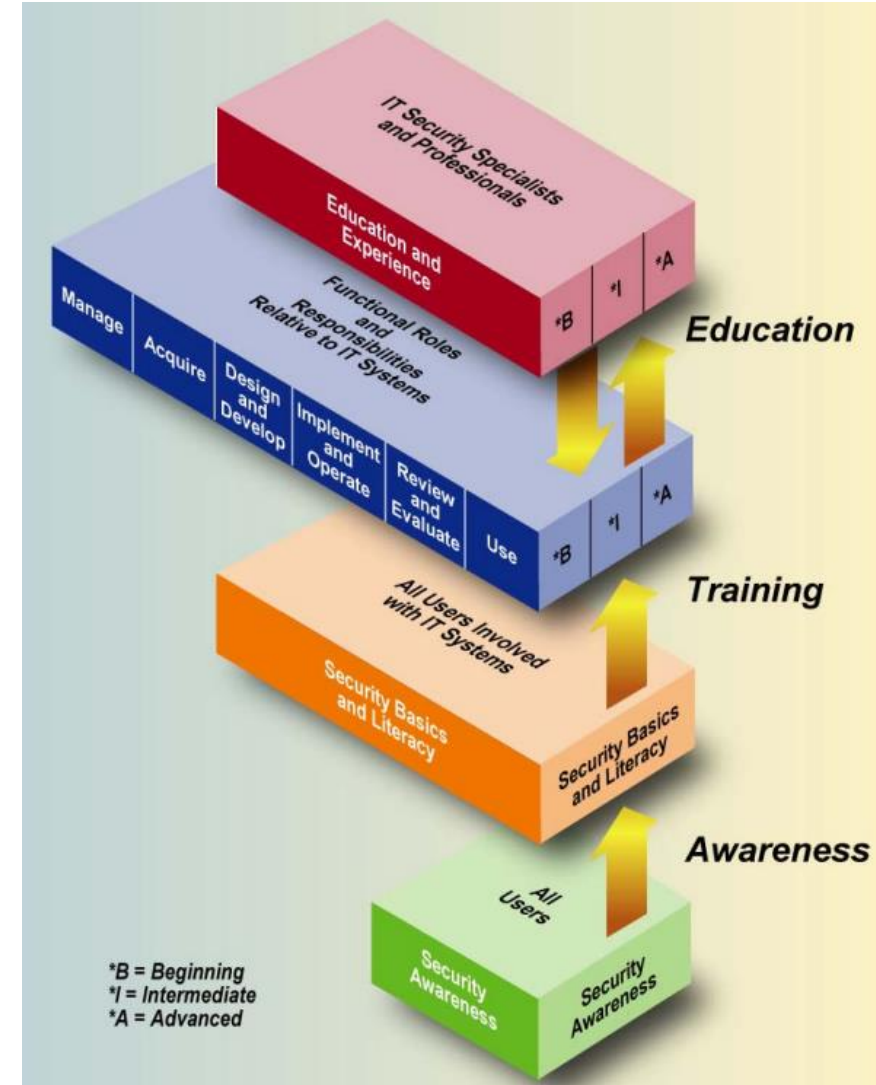
# In-Demand Skills

- Project management - PRINCE2 or PMBOK
- Education, training and awareness program design
- Strategic cyber planning
- Analyse policy and provide policy advice
- Developing guidelines and resources
- Understand legislation
- Flexibly lead, plan and manage large cross-functional teams
- Communication, negotiation and influencing skills
- Writing reports and making effective presentations
- Assess and manage cyber risk
- Develop responses to cyber breaches including practical operating models, playbooks and tools
- Analyse, design, implement, optimise and evaluate cyber response activities
- Develop, refine, review and refine cyber risk operating models
- Assess frameworks for cyber risk across functions including operational risk, regulatory risk, privacy, financial crime and compliance, deal risk and conduct risk.
- Provide GRC advice to SMEs and NFPs
- Develop and implement internal cyber strategy
- Conduct periodic cyber audits against standards including ISO27001, ITIL, COBIT5, NIST, PCI, PSPF, GDPR, HIPAA, FedRAMP, Essential 8, Mandatory 25, Consumer Data Right, with a view to certification where appropriate
- Develop cyber policies and procedures
- Present complex cyber ideas in simple language using productivity tools
- Develop short and long term cyber security roadmap
- Partner and collaborate with functional areas (Engineering, IT, Operations, Finance, HR etc) to improve cyber compliance
- Business analytics

# Career Pathways

- Lead Project Manager - Cyber
- Cyber Security Lead Trainer
- Senior Manager - Technology and Cyber Risk
- Director - Platforms & Cyber Security
- Director - Regulation and Strategy (Privacy)
- Information Security Officer
- Head of Information Security
- Continuous Improvement Security Principal
- Policy & Strategy Consultant - Cybersecurity
- Manager, Cyber Security & Compliance
- Assistant Director - Regulation and Strategy (Privacy)
- Alliance Lead - Cybersecurity & Digital Trust
- Principal Consultant - Security
- Senior Cyber Security Analyst - People & Process
- Head of Data & Information Security
- Advisor Cyber Security Risk & Advisory
- Senior Information Security Consultant
- Manager, Compliance, Tech and Cyber
- Cyber Security Partner
- Senior Manager Operational Technology Cyber Security
- Group Cyber Governance Manager
- Manager Risk and Control Enablement (Cyber Security)
- Program Director Cyber Security
- Lead Cyber Security Awareness and Education Officer

# Awareness and Training



# Summary

- Australia and Taiwan continue to be subjected to numerous cyber attacks
  - Need to consider “People and Process” as well as “Technology”
  - Education needed to build the cyber programs of the next decade
  - Awareness and training also needed at a broader level to ensure resilience

# THANK YOU!

