MIS761
Cyber Security Strategies

Dept. of Information Systems & Business Analytics

Deakin Business School

Week One – Unit Introduction

About Me

Dr Wilson Li

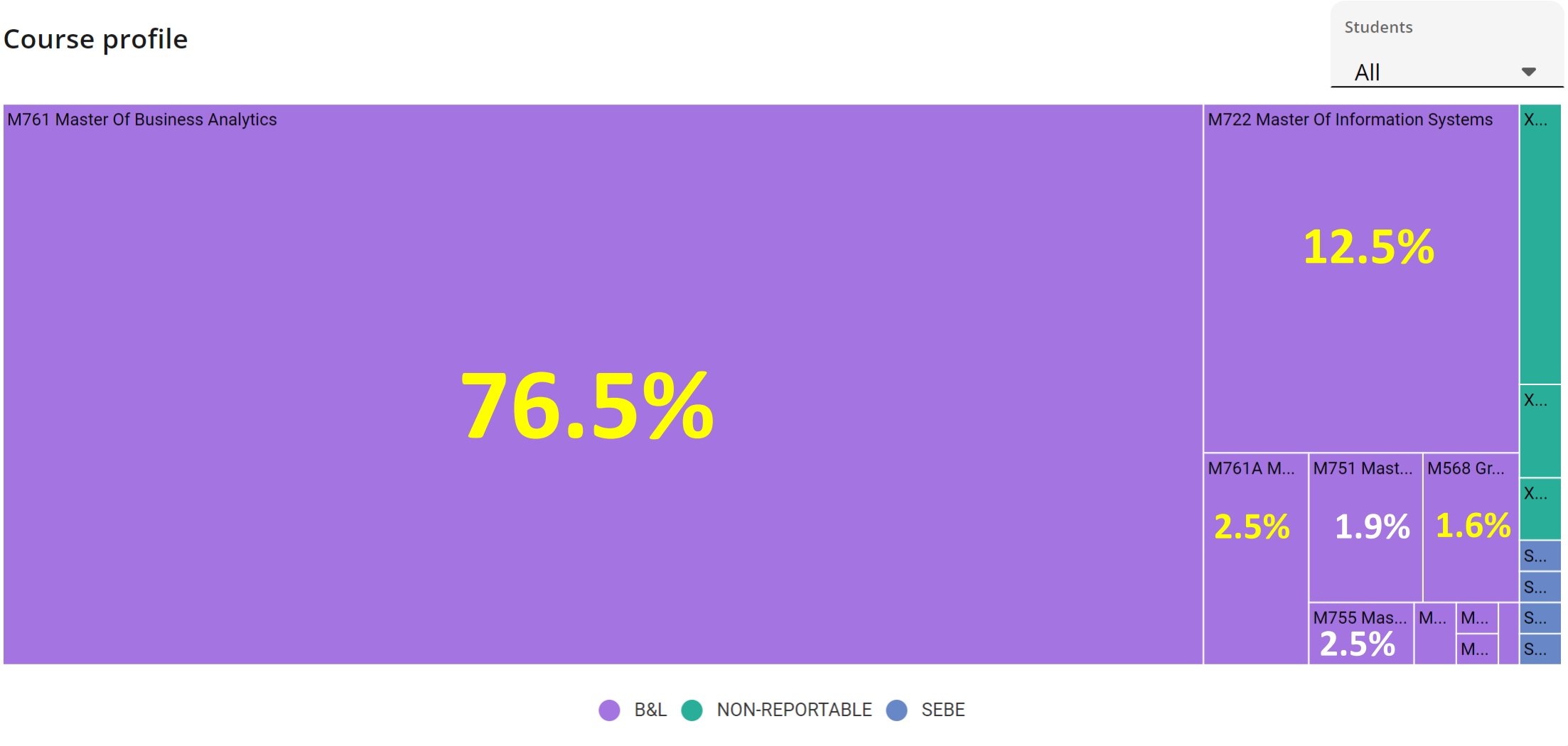
https://experts.deakin.edu.au/59096-Wilson-Li

Graduate Certificate in Higher Education (Learning and Teaching), Deakin University
Ph.D. (Information Systems), City University of Hong Kong
M.Sc. (Applied Economics), B.Eng. (Electronic Engineering)

Research Focus: Information Security, regulation, business value of IT
Research Method: empirical analysis
Recent works:
-To alert or alleviate? A natural experiment on the effect of anti-phishing laws on corporate IT and security investments
-A roadmap to achieving a healthier information ecosystem through GDPR implementation and privacy compliance technologies
-Where is IT in Information Security? The Interrelationship among IT Investment, Security Awareness, and Data Breaches

About You

Course profile



Teaching Team

Dr. Wilson Li - Unit Chair & Lecturer @ Burwood Campus and Online Campus
Dr. Sana Ansari & Dr. Abhishek Kumar Jha – Lecturers & Tutors @ GIFT Campus
Dr. Ishan Senarathna, Dr. Ruwan Nagahawatta, Dr. Anagi Gamachchi, Mr. Alex Zhang – Tutors @ Burwood Campus
Dr. Mohammad Belayet Hossain – Tutor @ Online Campus

Weekly Timetables Activities (Burwood & Online Campus)

Lectures:

- Tuesday 6pm-7:20pm in LT13 (HC2.005)on the Burwood Campus
- Class Lectures will be ***livestreamed via Zoom*** and ***recorded*** (links will be available on the unit site)***.***

Cloud Seminar for Cloud and Off-Shore Students:

- Wednesday 7pm-8:20pm (Melbourne Time) **via Zoom**;

this seminar will be **recorded** (links will be available on the unit site)

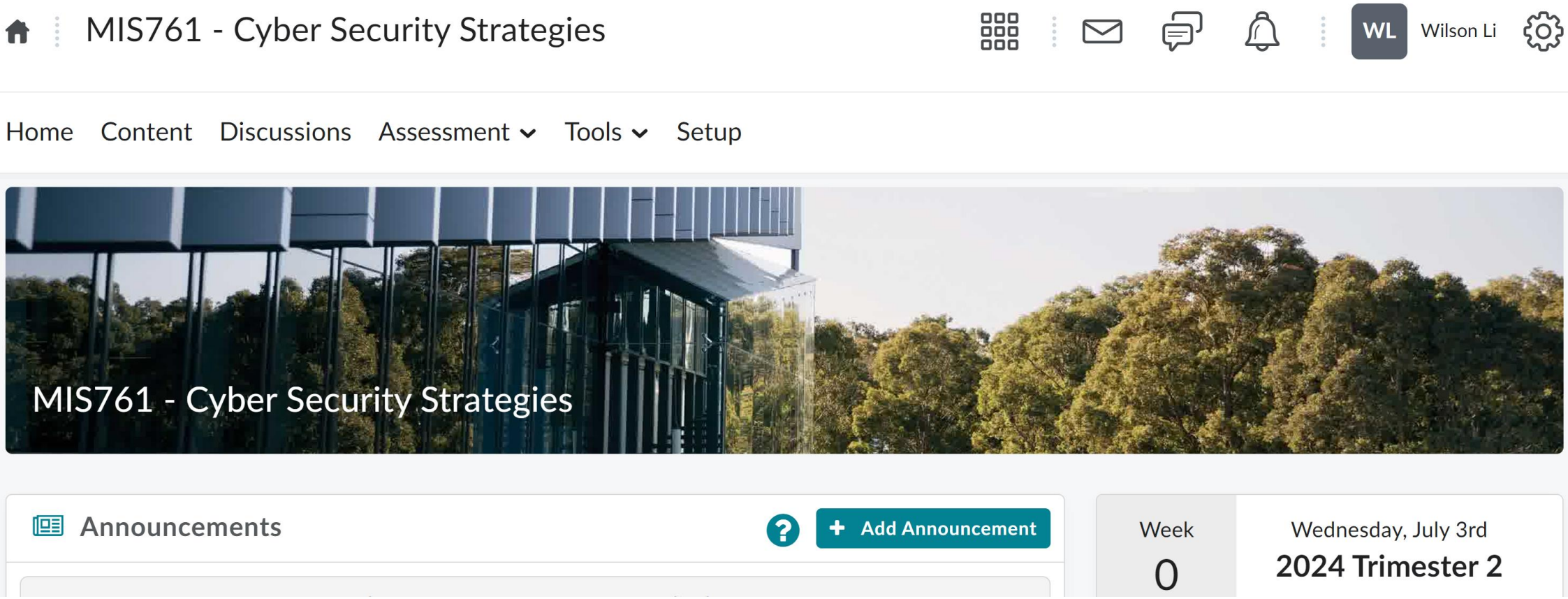
Weekly Timetables Activities

- **Burwood Campus Seminar:**
- Tue 19:30-20:50 at HD3.008 and HD3.009 (led by Ruwan & Alex)
- Wed 09:00-10:20, 10:30-11:50, 12:00-13:20 at HD3.009 (led by Anagi)
- Wed 14:00-15:20 at BC1.007 (led by Anagi)
- Wed 15:30-16:50 at BC1.007 (led by Alex)
- Wed 17:00-18:20 at BC1.007 (led by Ishan)
- Thur 18:00-19:20, 19:30-20:50 at LC5.107 (led by Ruwan)
- Fri 09:00-10:20 at LC4.101 (led by Alex)
- Fri 10:30-11:50 at LC4.101 (led by Anagi)

Getting Help …

- Post your questions on CloudDeakin (under relevant Discussion Forums)
- Ask for help in class and seminars
- Email the unit chair for personal matters
- Please let us know if you need help as soon as possible so that we can help you quickly! ☺

Introduction to the unit site



AACSB ACCREDITED

DEAKIN BUSINESS SCHOOL

Student Benefits

- ACS Student Membership
  - Network opportunities
  - Seminars/Workshops relevant to cybersecurity
- ASIA Student Membership
  - Australian Cyber Conference 2024 (26-28 NOVEMBER 2024)
    - Volunteer for one day and gain a full conference registration for FREE!
- Certified in Cybersecurity (CC) from ISC2
  - FREE Cybersecurity Training and Exam for a Limited Time
    - But we've secured at least 200 quotas for Deakin students!

Learning Activities & Resources

- ***Lectures –*** expect regular attendance.
  - Pre-lecture activities: questions to ponder with real-life examples
    - Padlet is anonymous: There is no stupid answers!
  - Slide Outline
  - Finalized Slides posted after lecture (no need to take photo☺)
- ***Seminars –*** participate and contribute to discussions, ask questions.
  - Pre-seminar activities: May need to source some cases
- ***Teaching staff*** – we are here to help and guide your learning, so just ask us.

Learning Activities & Resources

- ***CloudDeakin***:
  - Discussion areas – help each other here if you know the answer.
  - Class Recordings – a great way to refresh and revise.

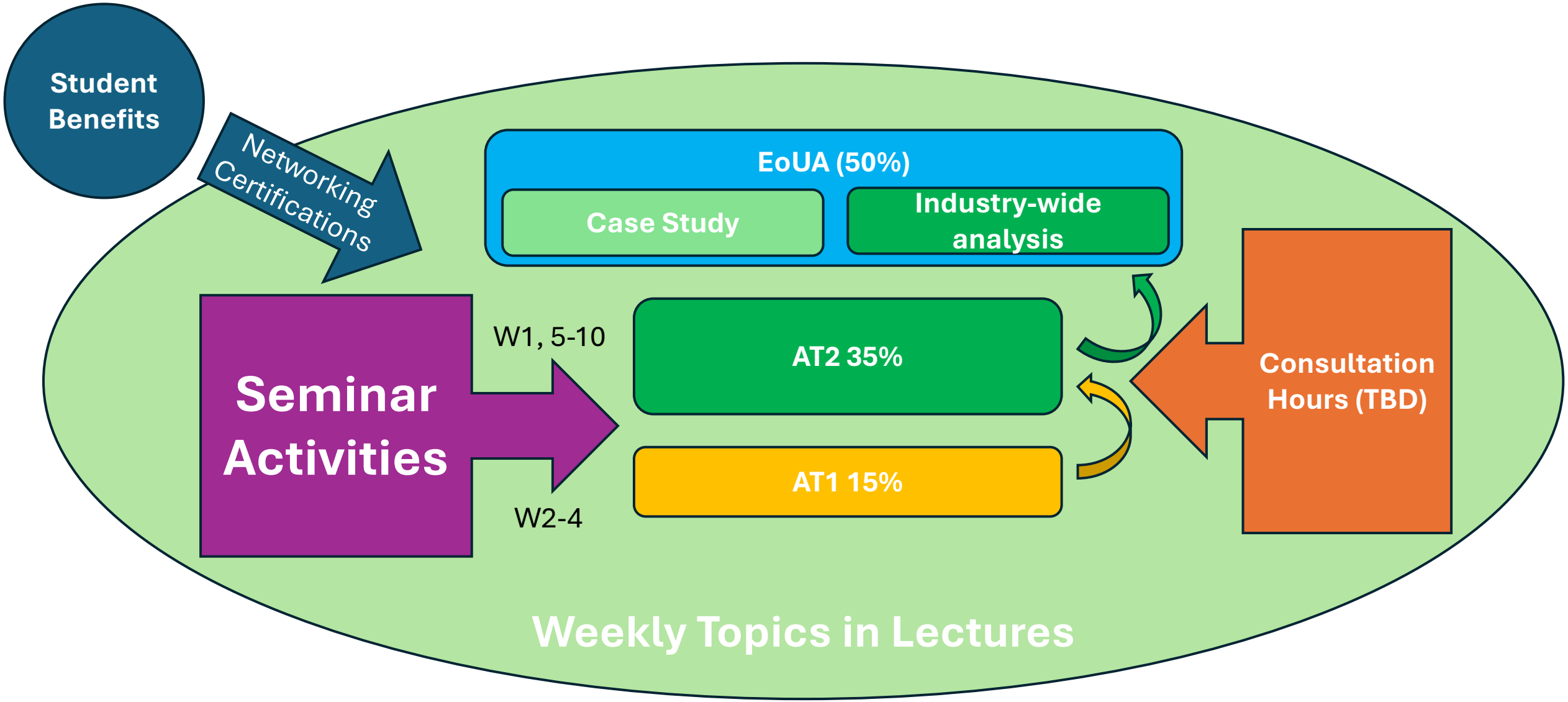
- ***Taking notes –*** a great habit to develop in Classes and Seminars.
- ***Deakin Library –*** ask a friendly Librarian, they love to help you.
- ***Discussions with class-mates -*** it helps to talk about stuff with your peers.
- ***Reference Books:***
  - Whitman, M.E. (2019) Management of information security
  - Whitman, M.E. (2021) Principles of Information Security

Assessments & Seminar Activities

- AT1 (15%, individual, 12min voice-over presentation) DUE @ W5
  - Design a security-awareness training artifact
  - Consider it as a chance to approach the potential entities in AT2
  - **Activities to help your preparation in Seminars from W2-4**
- AT2 (35%, group of 3, 3500-word business report) DUE @ W10
  - Self-source a real-life small-medium entity, no requirements on locations and industries
  - Conduct a cyber resilience review of the entity
    - **An interview questionnaire template based on NIST CSF 2.0 is available**
  - **Group formation activity in W1 Seminar**
  - **Guide you prepare the interview, and the report in Seminars from W5-10.**
- EoUA (50%, individual, open-book exam)
  - The exam will be schedule in one day during the exam period and available for 24 hours
  - You can start the exam at any time and submit your answer at any time during the 24-hour window.

AACSB ACCREDITED

DEAKIN BUSINESS SCHOOL


Student Benefits
Networking Certifications
EoUA (50%)
Case Study
Industry-wide analysis
Seminar Activities
W1, 5-10
W2-4
AT2 35%
AT1 15%
Consultation Hours (TBD)
Weekly Topics in Lectures

Weekly Topic Schedule

Week	Topic	Assessment due date
1	Introduction	
2	Cyber Threats and Their Business Impact	
3	Cyber Hygiene	
4	Technical Safeguards	
5	Risk Management	AT1 due 9 Aug 2024 at 8pm AEST
6	Legal, Ethical, and Compliance	
7	Incident Response and Business Continuity	
8	Cybersecurity Policies	
9	Cybersecurity Resilience	
10*	Cybersecurity Leadership	A2 due 20 Sep 2024 at 8pm AEST
11	Emerging Trends and Revision	

Let us Discuss a few Concepts

Security

Cyberspace

Cybersecurity

Strategy

…

MIS761
Cyber Security Strategies

Dept. of Information Systems & Business Analytics

Deakin Business School

Misconception of Cyber Security & Cyber Labor Shortage Issues

Misconception 1: Cybersecurity is a Technology Issue

From the perspectives of the business

- Outcomes
  - Business Disruption, Financial Losses and Brand Damage
    - AutoNation, Other Car Dealers Hurt by CDK Cyberattack as Outage Persists - WSJ
    - Western Sydney University discloses data breach, 7,500 'impacted individuals' notified - Cyber Daily
  - Regulatory Fines and Legal Repercussions
    - Microsoft Grilled on Capitol Hill Over Security Failures - WSJ
  - Creditworthiness-Impact on Financial Standing and Credit Ratings
    - Cyberattacks pose mounting risks to creditworthiness: Moody's | Cybersecurity Dive
  - Societal Impact-Broad Disruption to Essential Services
    - NHS says London hospitals cyber attack recovery could take months, calls on blood donors - Cyber Daily

Misconception 1: Cybersecurity is a Technology Issue

From the perspectives of the business

- Requirements from different stakeholders
  - Business partners (i.e., suppliers, vendors): Robust Security in Supply Chain Management
    - Businesses fear supply chain breach more than direct attacks - Cyber Daily
  - Regulators: Legal Compliance and Proactive Security Measures
    - OAIC files lawsuit against Medibank for 2022 data breach - Cyber Daily
  - Customers: Data Protection and Transparency
    - Storing unnecessary data? Expert issues stark warning - Cyber Daily
  - Societies: Global Cooperation and Economic Stability
    - Can Cybersecurity Be a Unifying Factor in Digital Trade Negotiations? (darkreading.com)

Misconception 1: Cybersecurity is a Technology Issue

From the perspectives of the business

- A comprehensive approach integrating culture, policy, and management practices beyond Technology
  - Cyber Hygiene/Culture
  - Compliance Management
  - Risk Management
  - Incident Response and Business Continuity
  - Cybersecurity Policies
  - Cybersecurity Resilience/Insurance
  - Cybersecurity Leadership

Misconception 1: Cybersecurity is a Technology Issue

From the perspectives of the adversaries

- Commoditization of Cyber Attacks
  - Hacking-for-Hire (or Hacking-as-a-Service): Professional hackers offer services for targeted attacks.
    - Ransomware-as-a-Service: Is RaaS becoming commoditised? - Information Age (information-age.com)
- Impact of Commoditization
  - Simplifies launching attacks
  - Increased frequency and sophistication of attacks.
  - High-profile cases like Elliott Management and Exxon show severe impacts.
- Business Strategies of Adversaries
  - ROI Calculation: Targeting weaker links for higher returns.
  - Innovation: Continuously evolving tactics to evade detection.
- Business Responses
  - Proactive and Dynamic Strategies: Regular updates, advanced threat detection.
  - Prioritize Defenses: Focus on high-risk industries and data types.

Misconception 2: Cybersecurity can be Considered Afterwards

- IT and Data are Everywhere, so as Risks
  - Traditional asset-centric security is outdated
  - Risks can emerge from any point in the network
  - ACMA says coding error to blame for Optus cyber attack - Cyber Daily
- Secure by Design Embedding security in the initial development stages
  - Reduces risk of costly breaches and post-deployment fixes
  - Integrating security into business processes and personnel practices
  - Ensures comprehensive protection across the organization
  - Inside the 'Secure By Design' Revolution (informationweek.com)
- Resilience: Prepare for the Worst
  - Combines IT security with business continuity to ensure continuous operation
  - Focuses on preparation, response, and recovery, acknowledging that cyber incidents may still occur despite best prevention efforts.
  - Why Cyber Resilience May Be More Important Than Cybersecurity (informationweek.com)

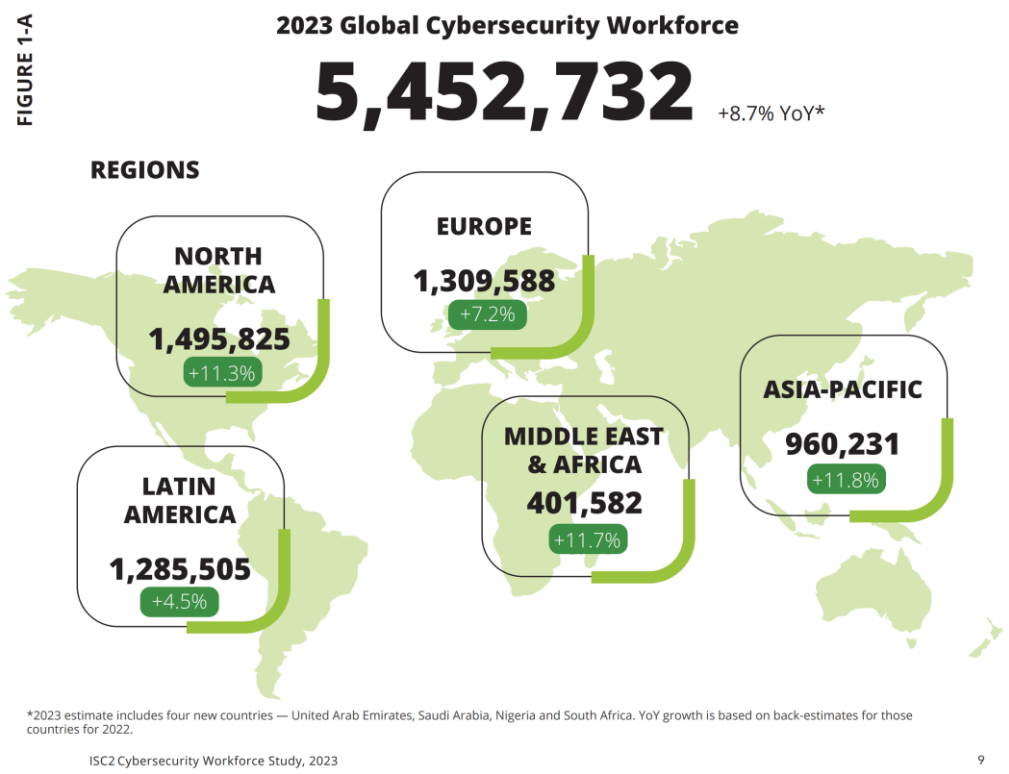
Misconception 3: Cybersecurity is a cost centre

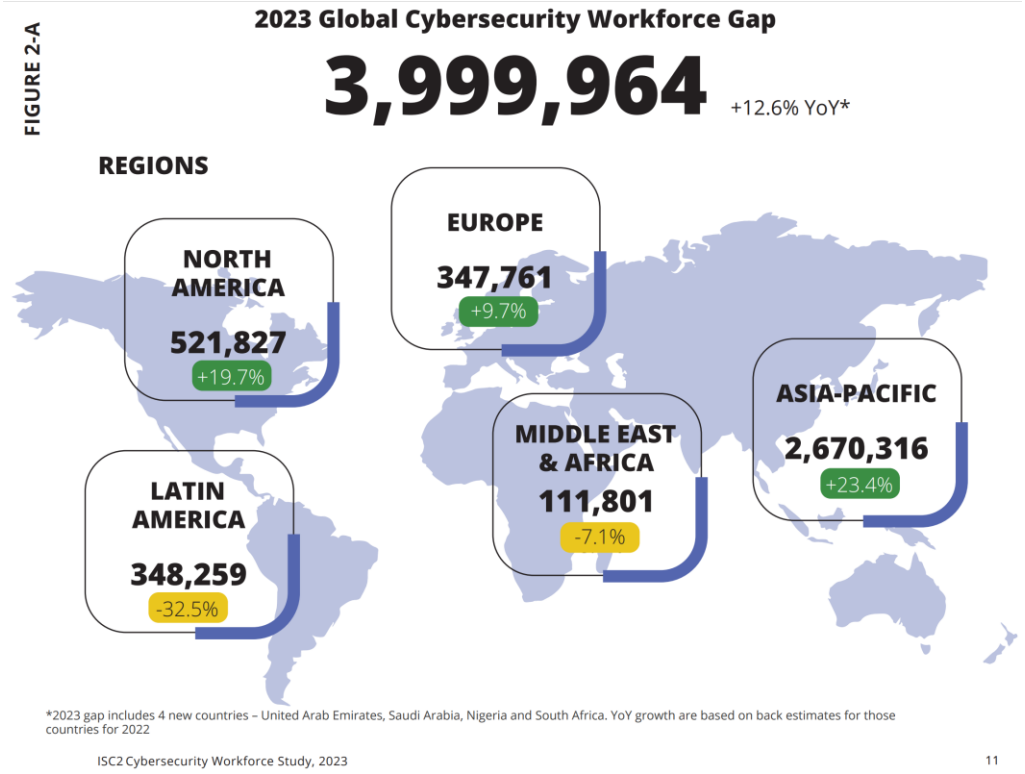
- Cybersecurity as a Competitive Advantage
  - Traditional cost centers (customer service, QA, R&D) now drive competitive advantage.
  - Cybersecurity enhances trust and customer engagement.
    - Bitdefender Scamio - Free Scam Detector
- Recognize and Align with Customer Needs
  - If customers value security, prioritize it.
    - ANZ signs up for ConnectID digital identity solution - Cyber Daily, ConnectID intro (youtube.com)
  - Educate customers to build loyalty
- Measure Cybersecurity Benefits
  - Enhancing Risk Management and Compliance
  - Improving Operational and Financial Performance
  - Building Customer Trust and Expanding Market Reach

Cyber Labor: A Big Gap

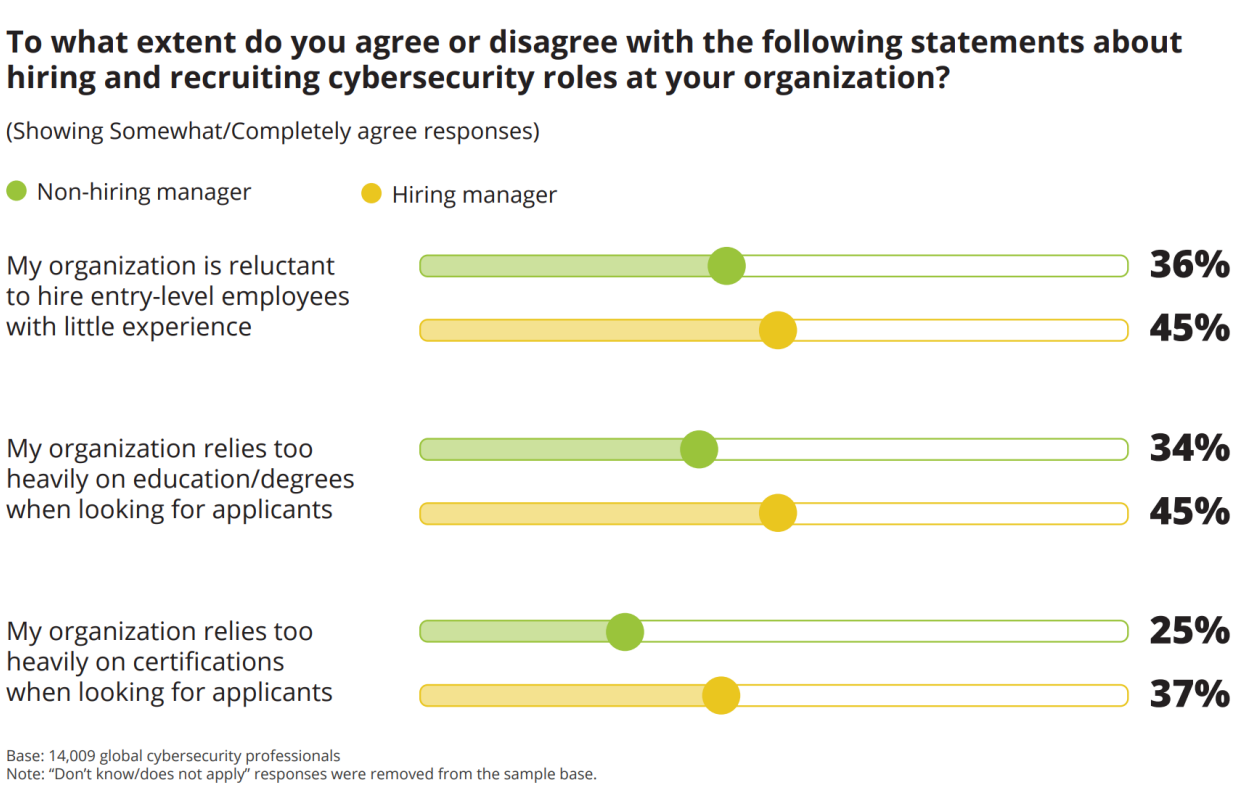
The Demand and Supply Fact *(Findings from ISC2)*

- **Global Workforce: 5.5 million (+8.7% YoY)**
- **Workforce Gap: 4 million (+12.6% YoY)**
- **Challenge: Demand outpacing supply despite workforce growth**

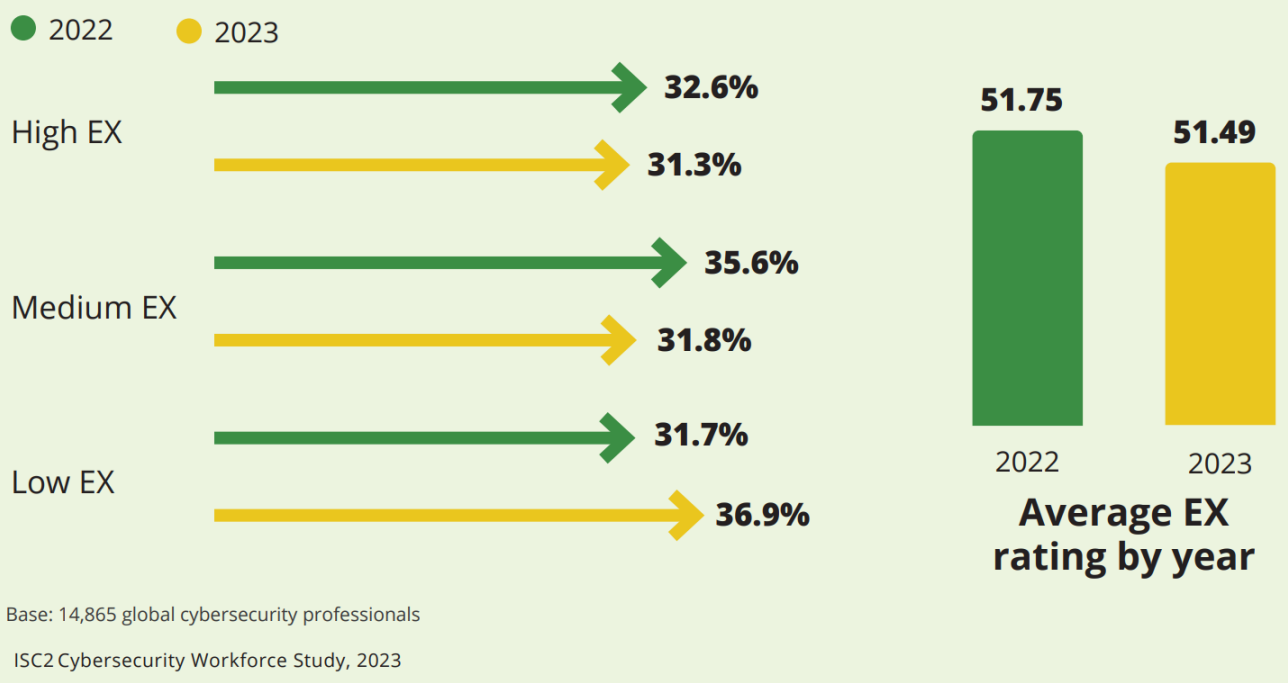




Cyber Labor: A Big Gap



- **Why go wrong?**
  - **Reluctance to Hire Entry-Level Employees**
    - 45% of hiring managers reluctant to hire entry-level
  - **Over-Reliance on Certifications and Degrees**
    - Emphasis on formal education and multiple certifications
  - **High Entry Barriers for New Professionals**
    - Extensive qualifications required for entry-level positions
  - **Perception of the "Perfect" Candidate**
    - Hiring managers holding out for ideal candidates

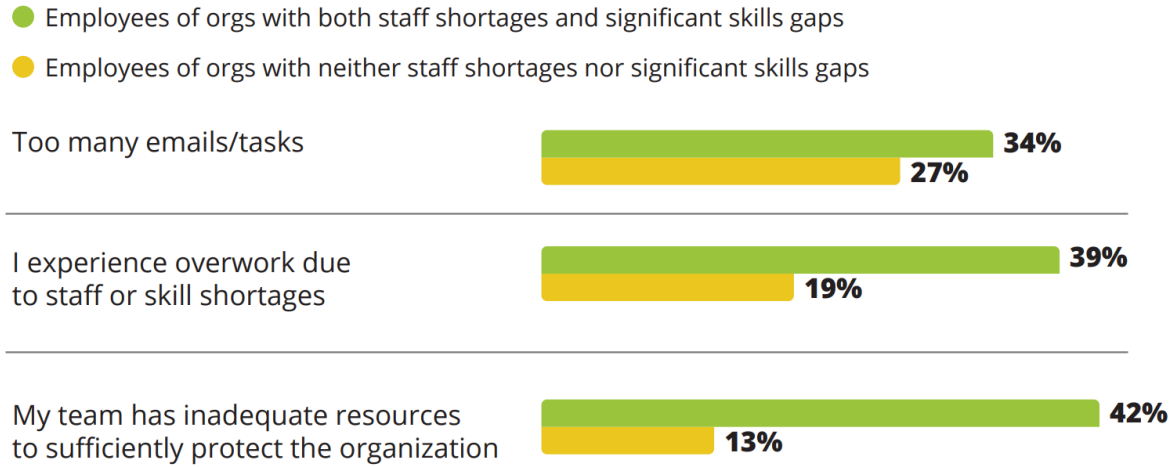


Base: 14,865 global cybersecurity professionals

ISC2 Cybersecurity Workforce Study, 2023

FIGURE 26

Which of the following are issues in your current role that negatively impact your job satisfaction?



Base: 4,172 global cybersecurity professionals.
Note: "Don't know/does not apply" responses were removed from the sample base.

A Vicious Cycle

Vicious Cycle of Labor Shortage and Burnout

- Significant labor shortage
- Increased Workload
- Burnout
- Turnover rates
- Disrupts security strategies
- Creates vulnerabilities in security infrastructure

Systemic Issues Contributing to Burnout

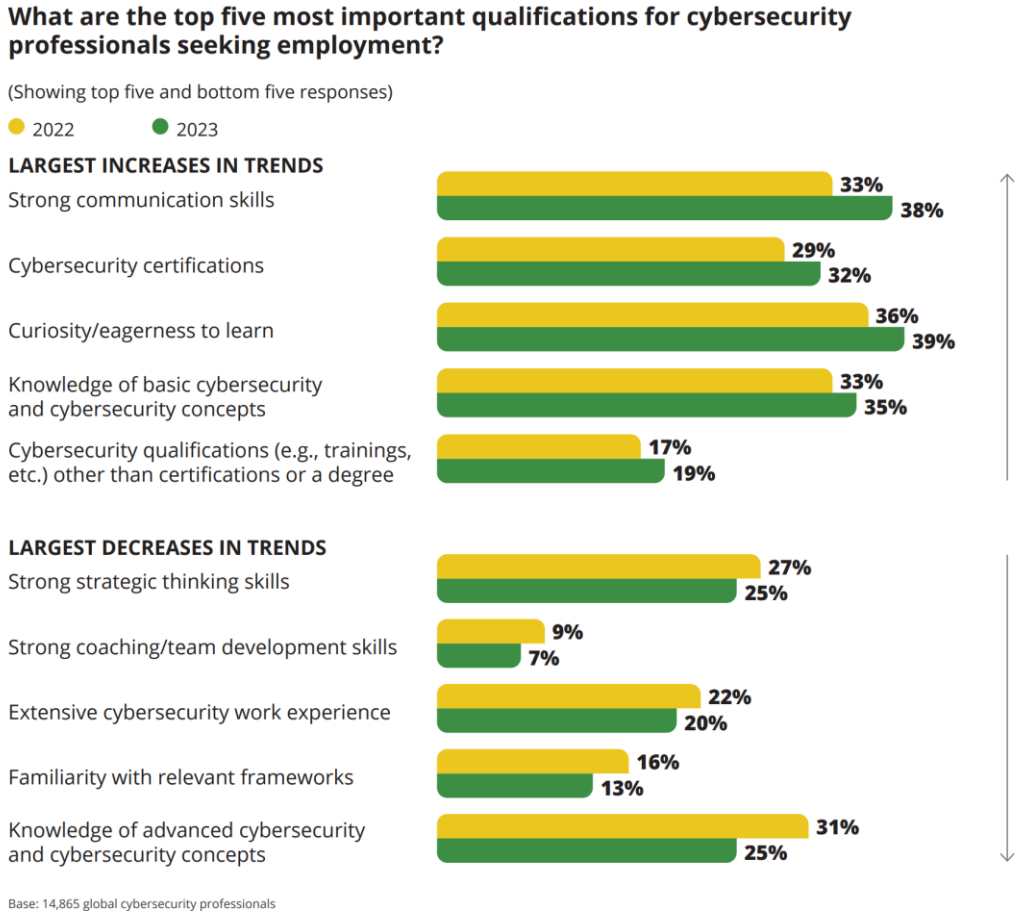
- Lack of support and inadequate tools decrease morale.
- Feelings of being unheard and unsupported by management.

Strategies to Break the Cycle

- Adopt sustainable staffing strategies.
- Foster a culture that values cybersecurity professionals' contributions.

Bridge the Gap – Credential-based to Skill-based

FIGURE 43



Broadening the Candidate Pool

- Expand beyond traditional credentials like degrees and certifications.
- Utilize non-traditional talent from various industries and demographics.

Reskill and Upskill

- Implement ongoing education and training to close skill gaps.
- Foster a continuous learning culture within the organization.

Embracing Alternative Pathways

- Recognize the value of non-traditional cybersecurity pathways.
- Increase internal recruitment efforts and value different career trajectories.

Leverage Technology

- Automated Operations
- Self-Service Tools
- Advanced Alert Management

Cybersecurity Career Frameworks

Response to Evolution: Developed due to the changing nature of cyber roles.

Skill Set Discrepancies: Address differences in skills for similar roles across employers.

Transparency & Standardization: Aim to bring clarity and uniformity to the cybersecurity sector.

Business Benefits: Facilitate workforce planning for businesses.

Candidate Benefits: Assist candidates in mapping out their career paths.

Regional Frameworks: UK, USA, AU, and EU have their distinct frameworks and focuses.

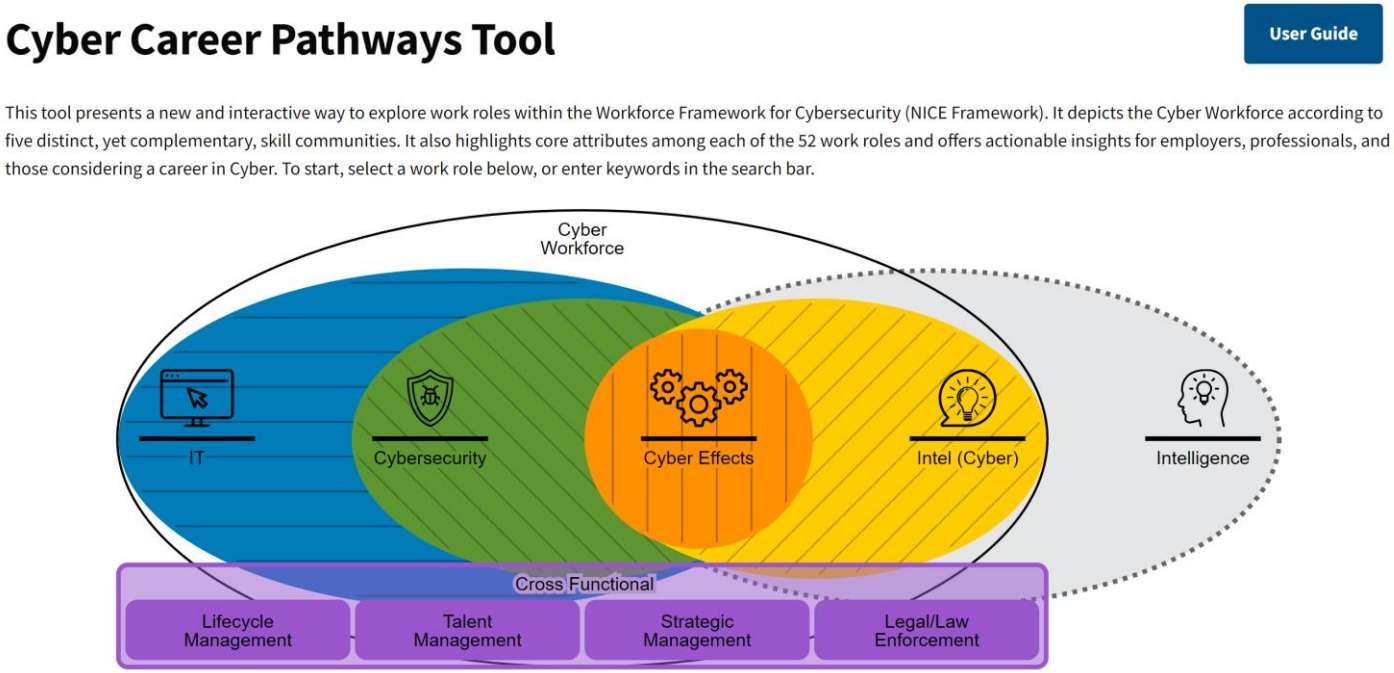
UK Cyber Career Framework

- Developed by the Cyber Security Council.
- Provides details about 16 specialisms in cybersecurity.
- Suggests pathways through and between these specialisms.
- Offers a flexible definition for practitioners to plan their careers.
- Each specialism includes:
  - Introduction to the specialism.
  - Typical responsibilities and tasks.
  - Required skills and knowledge.
  - Useful prior experience for entry.
  - Common job titles and average salary ranges.
- Aims to entice individuals from outside the sector to explore a career in cybersecurity.

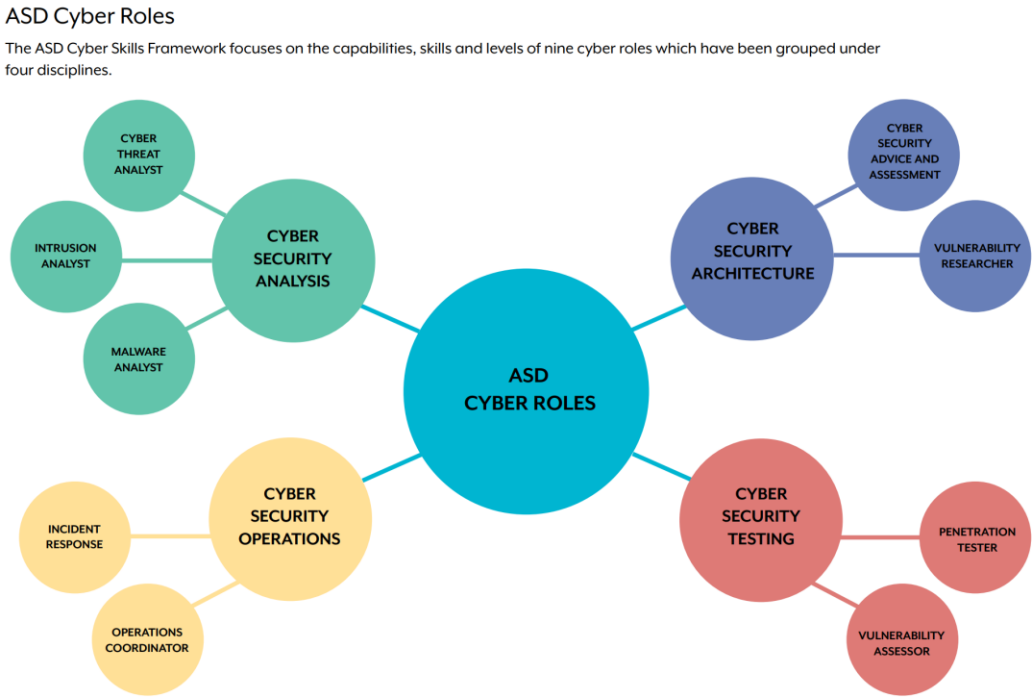
US NICE and the Cyber Career Pathways Tool

- **US NICE (National Initiative for Cybersecurity Education)**:
  - A partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development.
  - Aims to promote a robust network and ecosystem of cybersecurity education, training, and workforce development.
  - Provides a strategic framework to guide career development and workforce planning for the cybersecurity field.

- **Cyber Career Pathways Tool**:
  - Developed by the Cybersecurity and Infrastructure Security Agency (CISA) as part of the National Initiative for Cybersecurity Careers and Studies (NICCS).
  - Helps users identify, build, and navigate potential cyber career pathways.
  - Increases understanding of the knowledge, skills, and abilities needed to begin, transition, or advance in a cyber career.
  - Presents an interactive way to explore work roles within the NICE Cybersecurity Workforce Framework.
  - Depicts the cyber workforce as five distinct skill communities: IT, Cybersecurity, Cyber Effects, Intel (Cyber), and Cross Functional.
  - Offers actionable insights for employers, professionals, and those considering a career in cyber.



Australia Cyber Skills Framework



- Developed by the Australian Signals Directorate (ASD).
- Result of a comprehensive 2018 review.
- Reference Frameworks: Draws from CIISec Skills Framework, SFIA, and ILS.
- Implementation:
  - Creation of nine new occupational profiles within Defence and ASD.
  - Supports the Digital Transformation Agency in shaping cyber roles.
- In sync with Australia's Cyber Security Strategy 2020.
- Maps to the USA's NICE Cybersecurity Workforce Framework.
- Core Purpose: Standardizes and defines Australia's cyber roles and skills.

European Cybersecurity Skills Framework (ECSF)

- Overview: A practical tool to identify tasks, competences, skills, and knowledge associated with European cybersecurity roles.
- Reference Point: Defined in the Cybersecurity Skills Academy by the European Commission.
- 12 Profiles: The ECSF breaks down cybersecurity roles into 12 distinct profiles, detailing their responsibilities, skills, synergies, and interdependencies.
- Training Program Design: Supports the creation of cybersecurity-related training programmes.
- CyberHEAD: A database mapping ECSF role profiles to academic programmes, aiding students in making informed learning choices.
- Future Plans: The ECSF will play a pivotal role in the upcoming Cybersecurity Skills Academy, aiming to bridge the cybersecurity talent gap in the EU.

Certifications

ISC2	Certified in Cybersecurity (0yr, 2hr, FREE)	Certified Information Systems Security Professional* (have at least **five** years of **cumulative**, paid work experience in **two** or more of the eight CISSP domains)	Systems Security Certified Practitioner+ (have at least one year of cumulative work experience in one or more of the seven SSCP domains)
		Certified Secure Software Lifecycle Professional* (have at least **four** years of **cumulative**, paid work experience as a software development lifecycle professional in one or more of the eight CSSLP domains)	
ISACA	ISACA Cybersecurity Fundamentals (0yr, 2hr, U.S. $150)	Certified Information Security Manager* (Have **five** or more years of CISM professional work experience across at least **three** of the four CISM domains)	Certified Information Systems Auditor+ (Have **five** or more years of professional information systems auditing, control or security work experience)

*considered equivalent for skills, qualifications and experience for ACS Certified Professional (Cybersecurity) assessments
+ considered equivalent for skills, qualifications and experience for ACS Certified Technologist (Cybersecurity) assessments