Why does cyber security matter?

- Eight in 10 Australians access the internet daily and have social media accounts.
- Cybercrime is currently estimated to cost Australians more than $1 billion each year.
- Two-thirds of Australians don't read online privacy policies and almost half don't adjust their privacy settings on social media platforms.
- 46% of the world's population is connected to the internet.
- Global spending on cyber security is expected to almost double from around US$126 billion in 2016 to US$251 billion by 2026.
- International research and advisory firm Gartner Inc. predicts worldwide security spending will hit **$170 billion** in 2022, an 8% increase in just a year.

Why does cyber security matter?

- According to CISA, as of 2021, there is a ransomware attack every 11 seconds – a dramatic rise from every 39 seconds in 2019 (CISA Source). In addition, small businesses are the target of nearly 43% of all cyber attacks, which is up 400%.
- The average cost of a data breach is $3.92 million as of 2019.
- 57% of companies experienced social engineering or phishing attacks.
- 35% of data breaches involved internal actors.
- 1 in 36 mobile devices had high risk apps installed.
- 1 in 13 web requests lead to malware.
- 94% of malware is delivered via email
- 60 percent of breaches involved vulnerabilities for which a patch was available but not applied

Career paths and opportunities

- The Cyber Security average salary in Australia will range from $75000-$120,000 and they are always on the rise.
- According to its annual Cybersecurity Workforce Study, (ISC)² estimates the global gap in the workforce at over 4 Million

Cybersecurity roles and job Titles

- **Security Analyst:** analyzes and assesses vulnerabilities in the infrastructure (software, hardware, networks), investigates available tools and countermeasures to remedy the detected vulnerabilities, and recommends solutions and best practices.
- **Security Engineer:** Performs security monitoring, security and data/logs analysis, and forensic analysis, to detect security incidents, and mounts incident response.
- **Security Architect:** Designs a security system or major components of a security system and may head a security design team building a new security system.
- **Security Administrator:** Installs and manages organization-wide security systems. May also take on some of the tasks of a security analyst in smaller organizations.
- **Security Software Developer:** Develops security software, including tools for monitoring, traffic analysis, intrusion detection, virus/spyware/malware detection, anti-virus software, and so on. Also integrates/implements security into applications software.
- **Cryptographer/Cryptologist:** Uses encryption to secure information or to build security software. Also works as researcher to develop stronger encryption algorithms.
- **Cryptanalyst:** Analyzes encrypted information to break the code/cipher or to determine the purpose of malicious software.
- **Chief Information Security Officer:** a high-level management position responsible for the entire information security division/staff. The position may include hands-on technical work.
- **Security Consultant/Specialist:** Broad titles that encompass any one or all of the other roles/titles, tasked with protecting computers, networks, software, data, and/or information systems

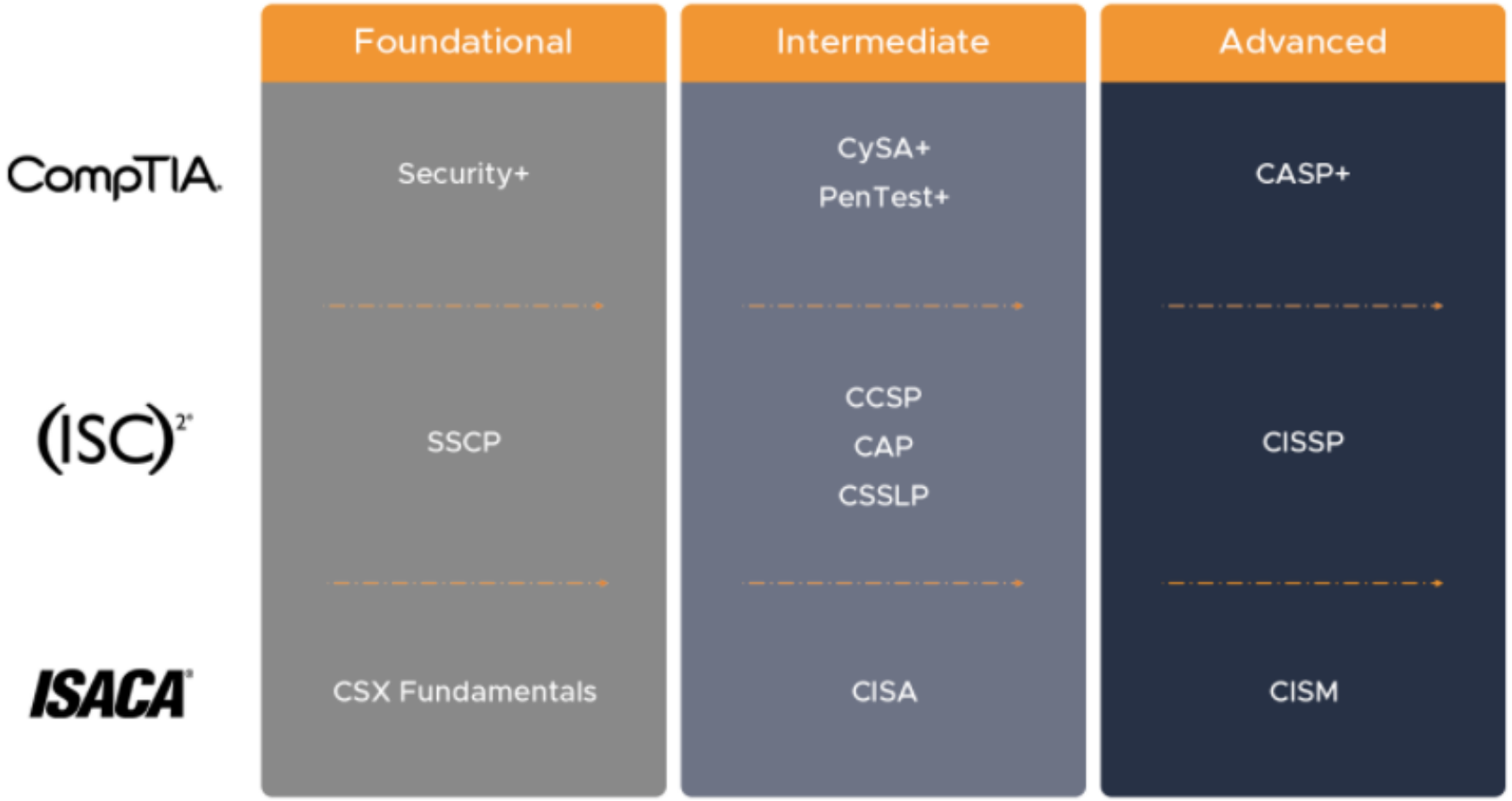
Very Specialized Roles

- **Intrusion Detection Specialist:** Monitors networks, computers, and applications in large organizations, looking for events and traffic indicators that signal intrusion.
- **Computer Security Incident Responder:** A member of team that prepares for and mounts rapid response to security threats and attacks such as viruses and denial-of-service attacks.
- **Source Code Auditor:** Reviews software source code to identify potential security issues and vulnerabilities that could be exploited by hackers to gain unauthorized access to data and system resources.
- **Virus Technician:** analyzes newly discovered computer viruses, and designs and develops software to defend against them.
- **Penetration Tester (also known as Ethical Hacker or Assurance Validator):** Not only scans for and identifies vulnerabilities, but exploits them to provide hard evidence that they are vulnerabilities.
- **Vulnerability Assessor:** Scans for, identifies and assesses vulnerabilities in IT systems including computers, networks, software systems, information systems, and applications software.

Typical Employers of Cybersecurity Graduates

- Technology and Internet companies
- Security software companies
- Defense companies
- Many government departments and defense/intelligence agencies
- Many IT companies, and IT divisions of companies in many industry sectors
- The E-Commerce sector
- Banks, financial firms, credit card companies
- And much more

Best cyber security certification path



Find the right job in cybersecurity

- ITJobMatch – The ITJobMatch search engine specializes in IT jobs of every kind, all over the globe.
- Monster – Monster is a search engine for all types of jobs
- CareerBuilder – CareerBuilder is also a search engine for all types of jobs.

Assessments

- 4 online quizzes - 60%
- Final case study report – 40%

Subject Schedule

	Topics and Activities
Day 1	Why does cyber security matter Cybersecurity – A World of Experts and Criminals Common Threats and Attacks Lab environment set up – Install VMware player and Ubuntu Linux and Cisco Packet Tracer
Day 2	Linux OS walkthrough
Day 3	OSI and TCP/IP model review
Day 4	Security Devices and Services – Firewall/IPS/ACL Quiz 1
Day5	Attacking the Foundation -TCP/UDP/IP Vulnerabilities
Day6	The Cybersecurity Cube The art of protecting secret, integrity, and availability Quiz 2
Day7	Cryptography
Day 8	Endpoint security Quiz 3
Day 9	Digital Forensics and Incident Analysis and Response
Day 10	Case Study Report Quiz 4 and final report

Need Help

- Add me as Wechat friend
- Email: yingying.yang@uts.edu.au