Cyber Security Essentials

Griffith University

Griffith UNIVERSITY
Queensland, Australia

All materials and recordings are not to be copied, shared or made public in any way.

All tools/methods learnt from this course are not to be used for any illegal purpose.

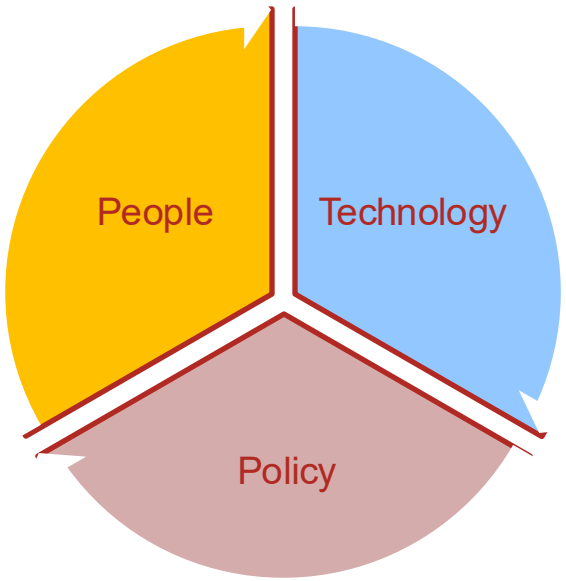
Griffith UNIVERSITY
Queensland, Australia

Course Objectives

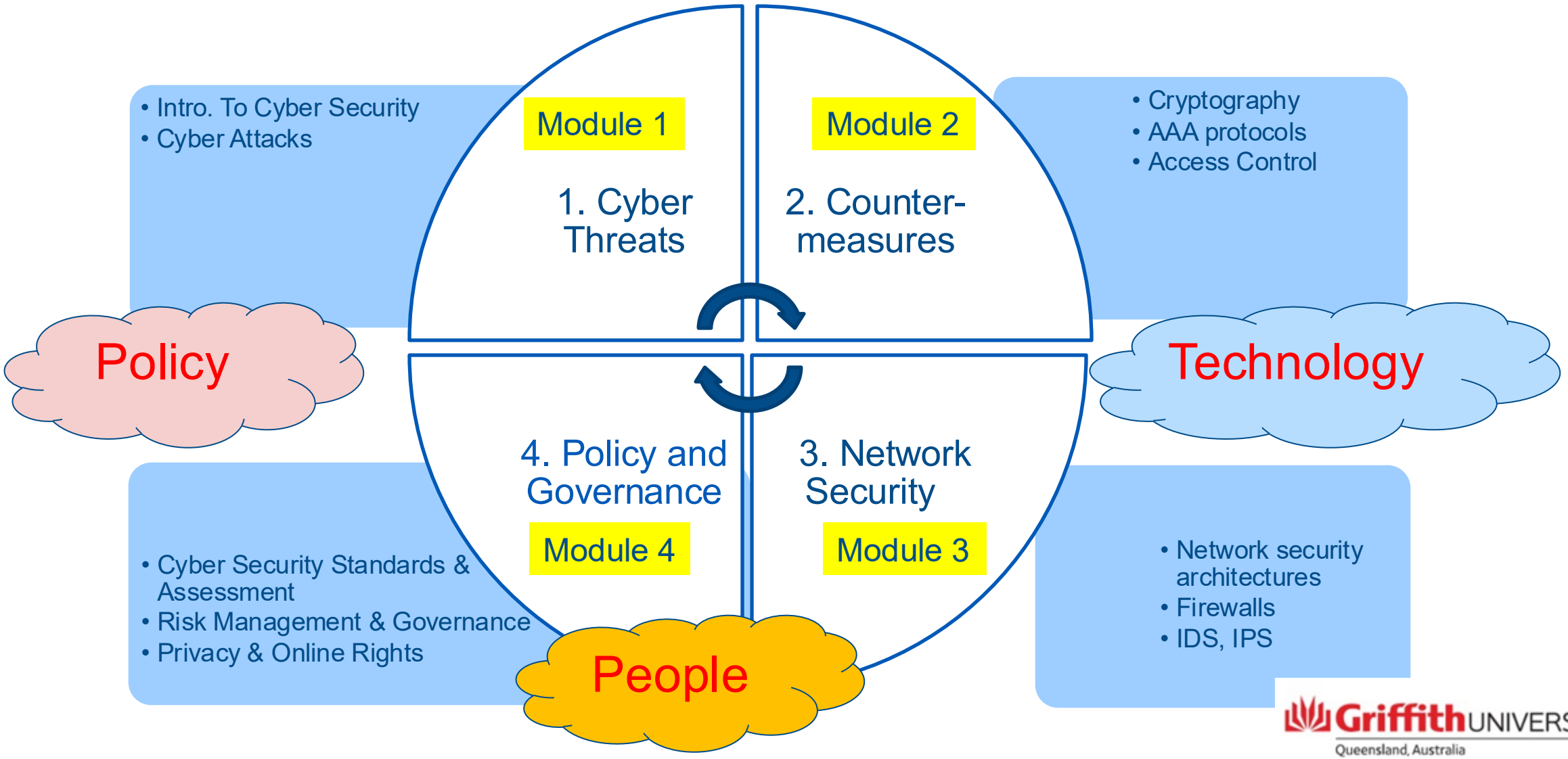
- Who “bad guys” are and what methods they use?

  Various cyber attacks and their impact on an organization’s capacity to accomplish its stated mission

- How to protect cyberspace?
  - ✓ Technology
  - ✓ Policy
  - ✓ People



Course Contents



Griffith UNIVERSITY
Queensland, Australia

	Lecture	Workshop
Week 1	Introduction to cyber security	No workshop
Week 2	Cyber Attacks	Linux Introduction
Week 3	Cryptography I	Symmetric Encryption (5%)
Week 4	Cryptography II	RSA (5%)
Week 5	Authentication protocols	SSH authentication (5%)
Week 6	Access Control	OS access control (5%)
Week 7	Network security I	Wireshark sniffing (5%)
Week 8	Network security II	Sniffing and Spoofing (5%)
Week 9	Privacy and Online rights	Privacy Impact Assessment –Assignment (15%)
Week 10	Social engineering and Security Awareness	Essential 8 study (5%)
Week 11	Risk Management and Governance	Case study
Week 12	Review	No workshop

Course Structure (7905ICT)

Week 1-12:

- Pre-lecture recording
- 1-hour lecture per week
- 2-hour workshop (No workshop in Week 1 & 12)

Assessment:

- 35% 7 Workshop quizzes
- 15% Case study assignment
- 50% Final exam (40/100 hurdle)

Course Arrangement

1. Lecture OL: 2pm-2:50pm Mon via Collaborate
2. Workshop in Week 2-11
   – SB&OL: 3pm-4:50pm Tuesday
3. Teaching team

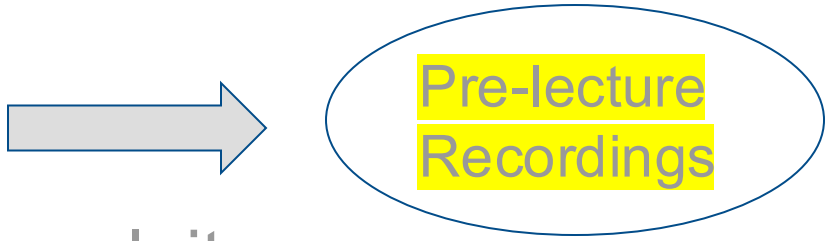
Ernest Foo (SB&OL), e.foo@griffith.edu.au, Tel: 07-37353681

Textbooks

- No textbook
- Reference books:
  - CISSP (All in one) exam guide, Shon Harris, Fernando Maymi, Eighth edition
  - Computer Sec. Principles and Practice 2nd Ed., W. Stallings and L. Brown (CSPP)
  - Cryptography and Network Security: Principles and Practice, 6th ed., William Stallings (CNS)
  - Computer Security, Wenliang Du, 2017
  - From CIA to APT: An Introduction to Cyber Security by Edward G. Amoroso , Matthew E. Amoroso
  - TCP/IP Illustrated Volume 1 (2nd Edition), Kevin Fall and W. Richard Stevens
- Recommended:
  - Ted “cybersecurity” videos
  - CompTIA
  - https://www.khanacademy.org/
  - CISSP (Certified Information Systems Security Professional) or other certificates

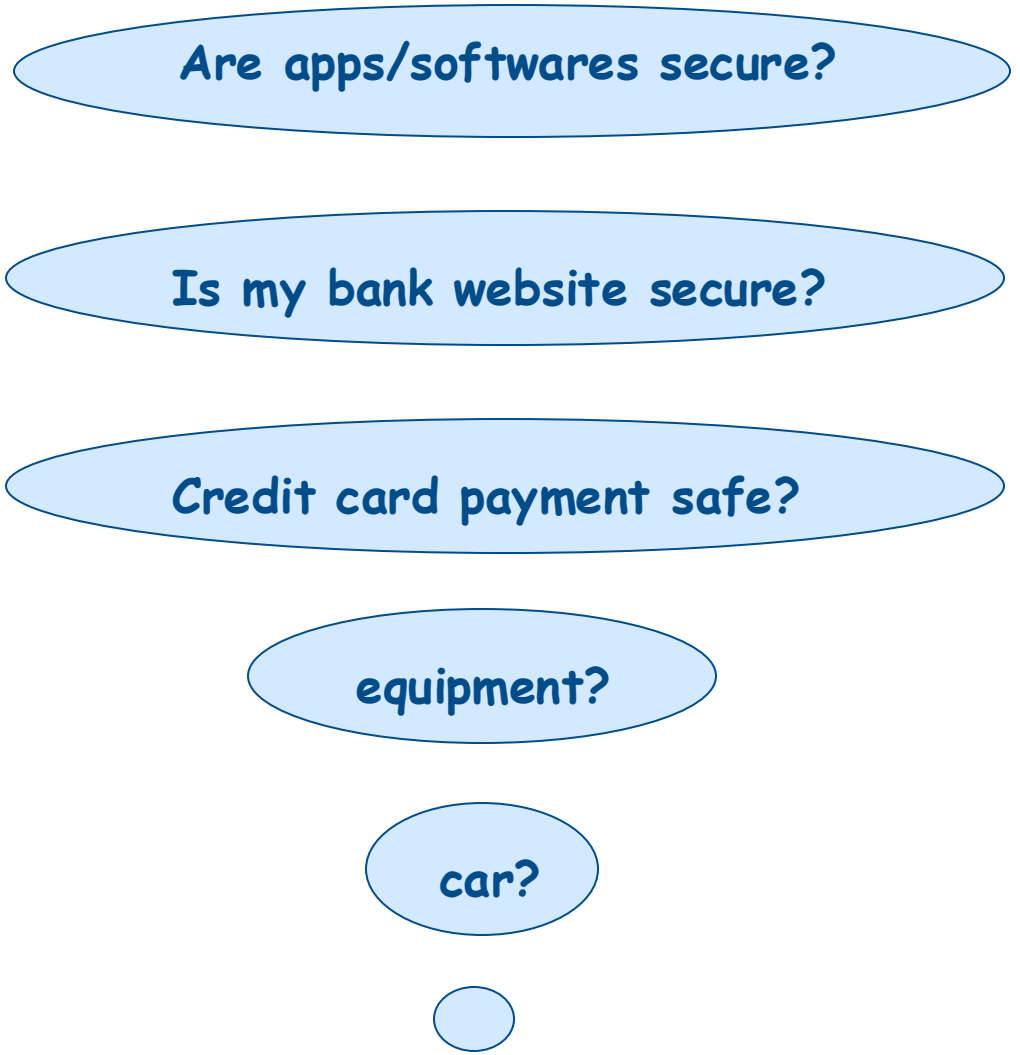
Mod 1-1 Outline

- Basics in Cyber Security
  - CIA model
  - Risks, threats, vulnerabilities, exploits

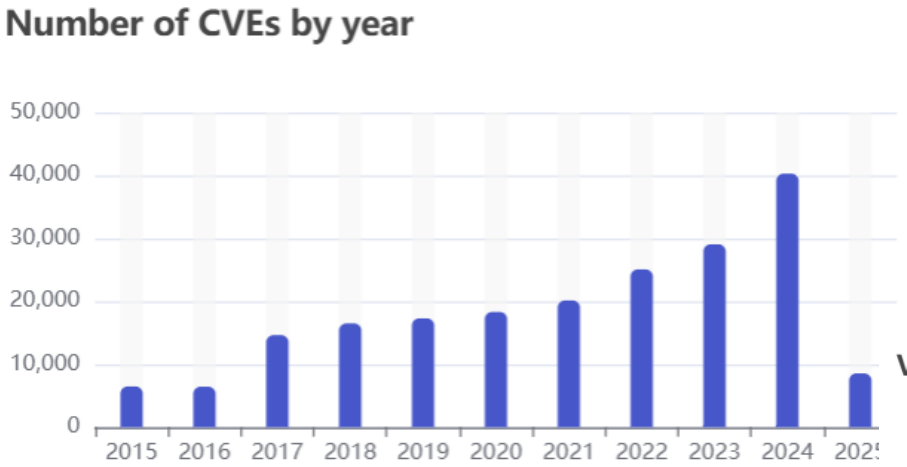


- Why study Cyber Security?
- Why does cyber crime exist?
- Career options

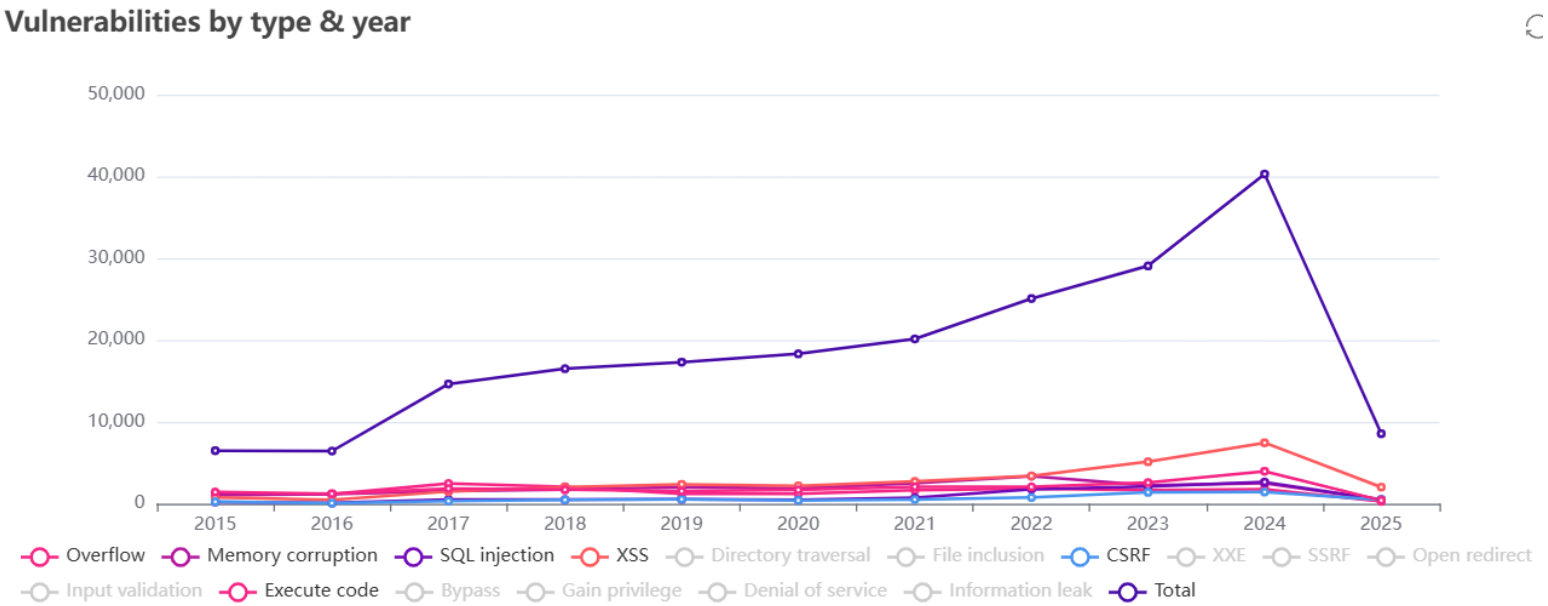
Why study cyber security?



Why study cyber security?



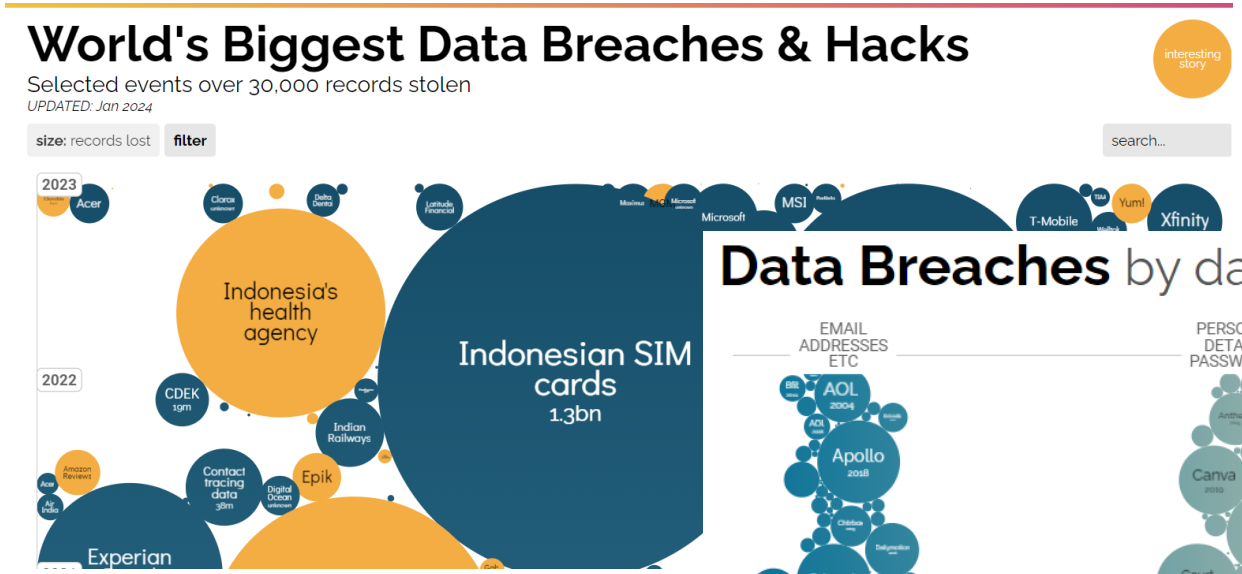
Are apps/software secure?

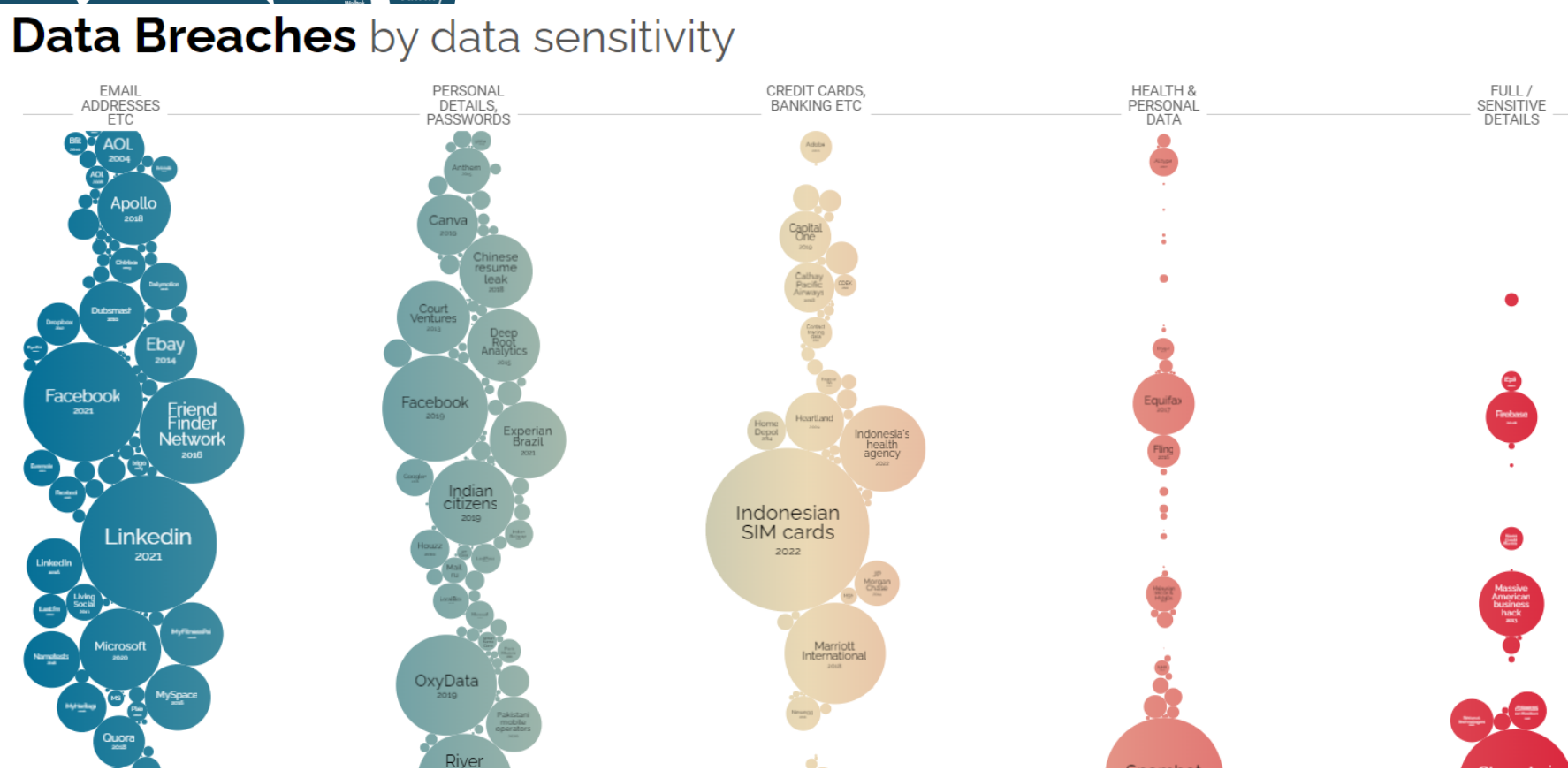


https://www.cvedetails.com/browse-by-date.php

Why study cyber security?

Is my bank website secure?





http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Why study cyber security?

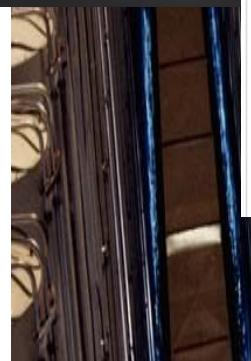
Equipment? Car?

https://www.youtube.com/watch?v=UbD51wG04bs

Hacking risk leads to recall of 500,000 pacemakers due to patient death fears

FDA overseeing crucial firmware update in US to patch security holes and prevent hijacking of pacemakers implanted in half a million people

Hackers Remotely Kill a Jeep on a Highway | WIRED



Cyber Data Breaches --- Top 10 (2021-2022)

Org/comp	breaches	How	when	who
Rockstar	game source code	employeeSlack account	Sep 2022	
Uber	System & customers data	Employee Slack account	Sep 2022	LAPSUS$
Red Cross	Personal data	3rd-party contractor	Jan 2022	
Credit Suisses	30,000 Swiss banks customers (where the money is from and why accepting)		Feb 2022	
Cash App	8.2M customer records	disgruntled employee	Dec. 2021	
Revolut	50150 customers records	3rd party access	Sep 2022	
Neopets	69M users, 460MB compressed source code (selling for 4 bitcoins online)	18 months access to IT systems	01/2021-07/2022	
Microsoft	37GB source code data incl. Bing, Bing maps … 250 projects in 9GB, 65K entities from 111 countries	Torrent, misconfigured server accessible online	Sep-Oct 2022	LAPSUS$ …
New York city department of education	820K students info	Unencrypted data in storage	Mar 2022	
South African Credit Bureau TransUnion	3M South African households, 600K business, 4TB clients data incl. passport, employers' id, spouse info, credit score	Ransomware asking for $15m ransom	Mar 2022	Brazilian N4aughtysec

Why study cyber security?

Cyber Security Workforce gap

(ISC)2 (the world's largest nonprofit association of certified cybersecurity professionals) – announced the findings of the Oct 2023 --- a widening of the global cybersecurity workforce gap.

The current global workforce gap is estimated to be 3,999,964 while the workforce itself is estimated to be 5,452,732, according to ISC2.

Australian Cyber Security Strategy (Released on 22 Nov. 2023)

https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf

The Strategy is the roadmap that will help realise the Australian Government's vision of becoming a world leader in cyber security by 2030.

To achieve this vision, we need to protect Australians. Through the Strategy we seek to improve our cyber security, manage cyber risks and better support citizens and Australian businesses to manage the cyber environment around them. We will do this with six cyber shields.

1. Strong businesses and citizens
2. Safe technology
3. World-class threat sharing and blocking
4. Protected critical infrastructure
5. Sovereign capabilities
6. Resilient region and global leadership.

The Australian Government's 2023-2030 Cyber Security Strategy, backed by a $586.9 million investment, marks a significant step towards fortifying Australia's digital landscape.

AustCyber

- **Severe shortage** of job-ready cyber security workers
- **Nearly 17,000** more cyber security workers needed by 2026

Griffith UNIVERSITY
Queensland, Australia

Why study cyber security?

- What will you learn?

90% of security incidents are caused by PEBCAK

Problem **E**xists **B**etween **C**hair and **K**eyboard

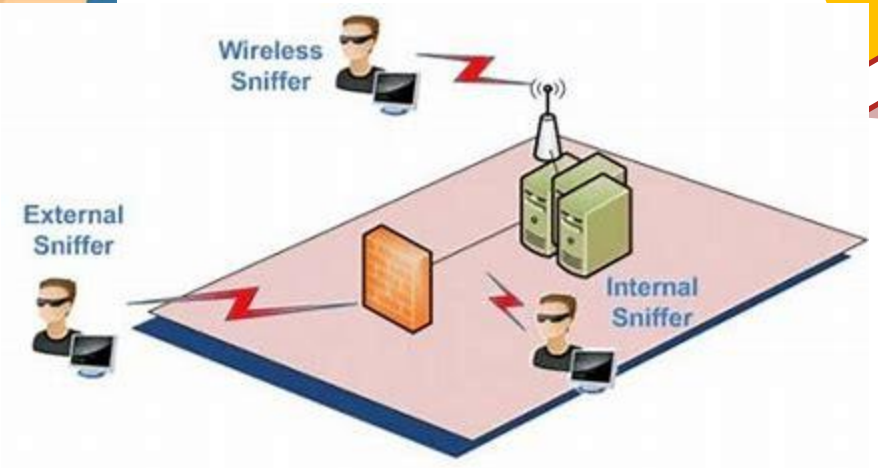
If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

--- Bruce Schneier, *Secrets & Lies*

Australian Government
Australian Signals Directorate

ACSC
Australian Cyber Security Centre

Essential 8



People

Technology

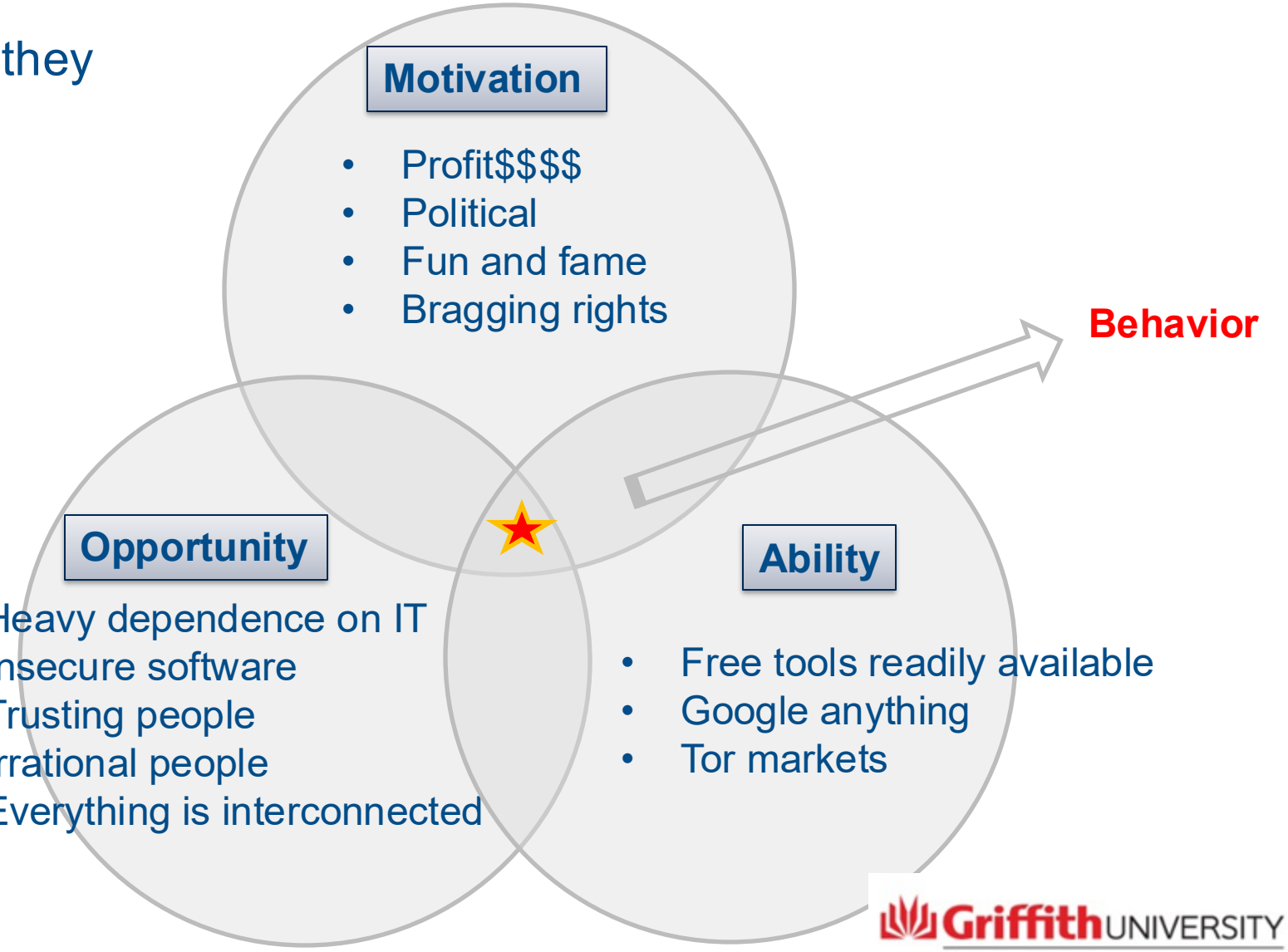
Policy

Cyber security standard
Cyber awareness training

Griffith UNIVERSITY
Queensland, Australia

Why does Cybercrime exist?

What did they do with the data they compromised?



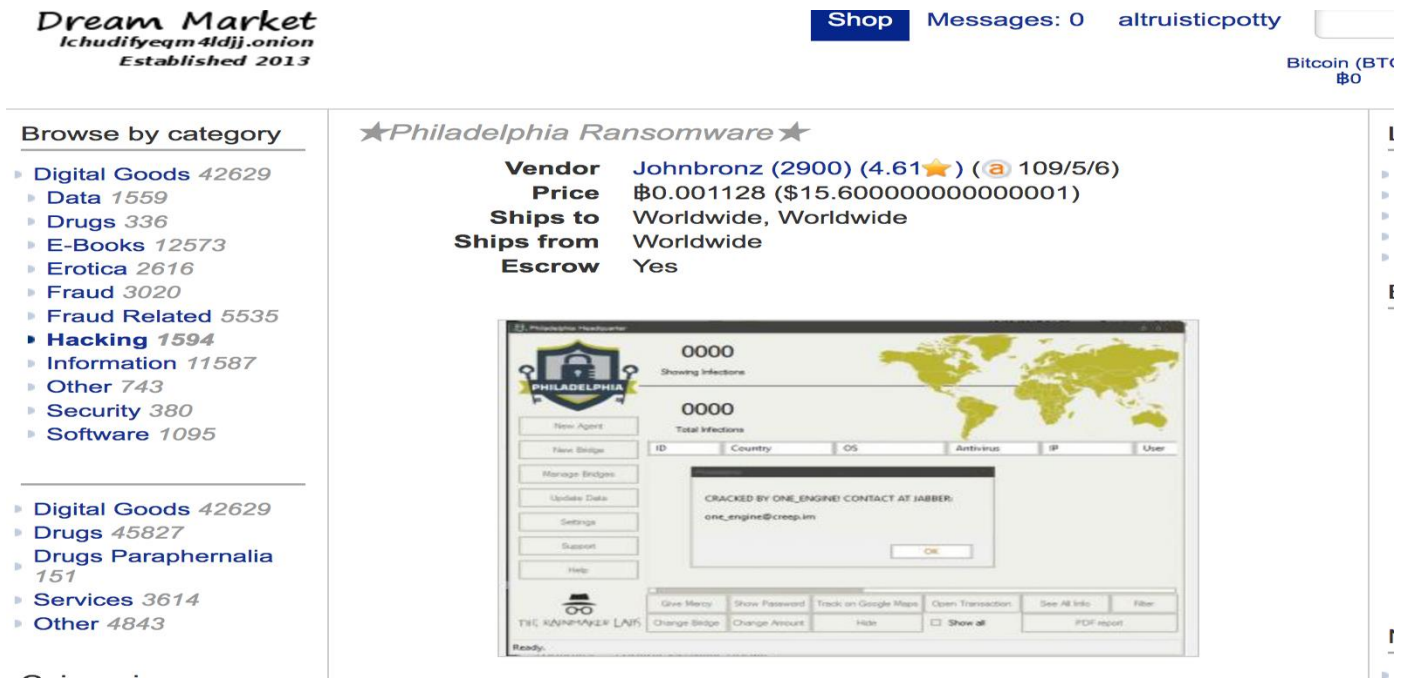
MAO Framework

Griffith UNIVERSITY
Queensland, Australia

Why does Cybercrime exist?

Why can attackers win?

- Asymmetric threat
- Insecure software/systems
- Human remains vulnerable



Exploit Toolkits on Tor Marketplace

Griffith UNIVERSITY
Queensland, Australia

Why does Cybercrime exist?

How to protect our data, network, systems?

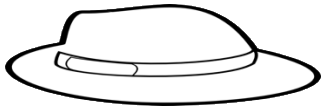
If you know both yourself and your enemy, you can win "a hundred" battles without jeopardy. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.

Sun Tzu –The Art of War

Who they are?

Their motivation?

How do they get in?



Black Hat Hacker = Crackers / Criminals
Engages in illegal activities for personal gains

White Hat Hacker = “Ethical” Hackers
Stays within the limit of the laws to fight cybercrime

Grey Hat Hacker = Somewhere in between
Engages in illegal activities, but not with malicious intent

Griffith UNIVERSITY
Queensland, Australia

How to become a cyber security professional?

VERY Broad knowledge

Operating Systems

Programming Languages

Hacker Methods

TCP/IP Networking

CPU Architecture

Security Tools

Cryptography

Computer Hardware

Security Standards

Information Security Management

Software Development

Risk Management

Security Engineering/Architecture

Auditing

Laws and Regulations

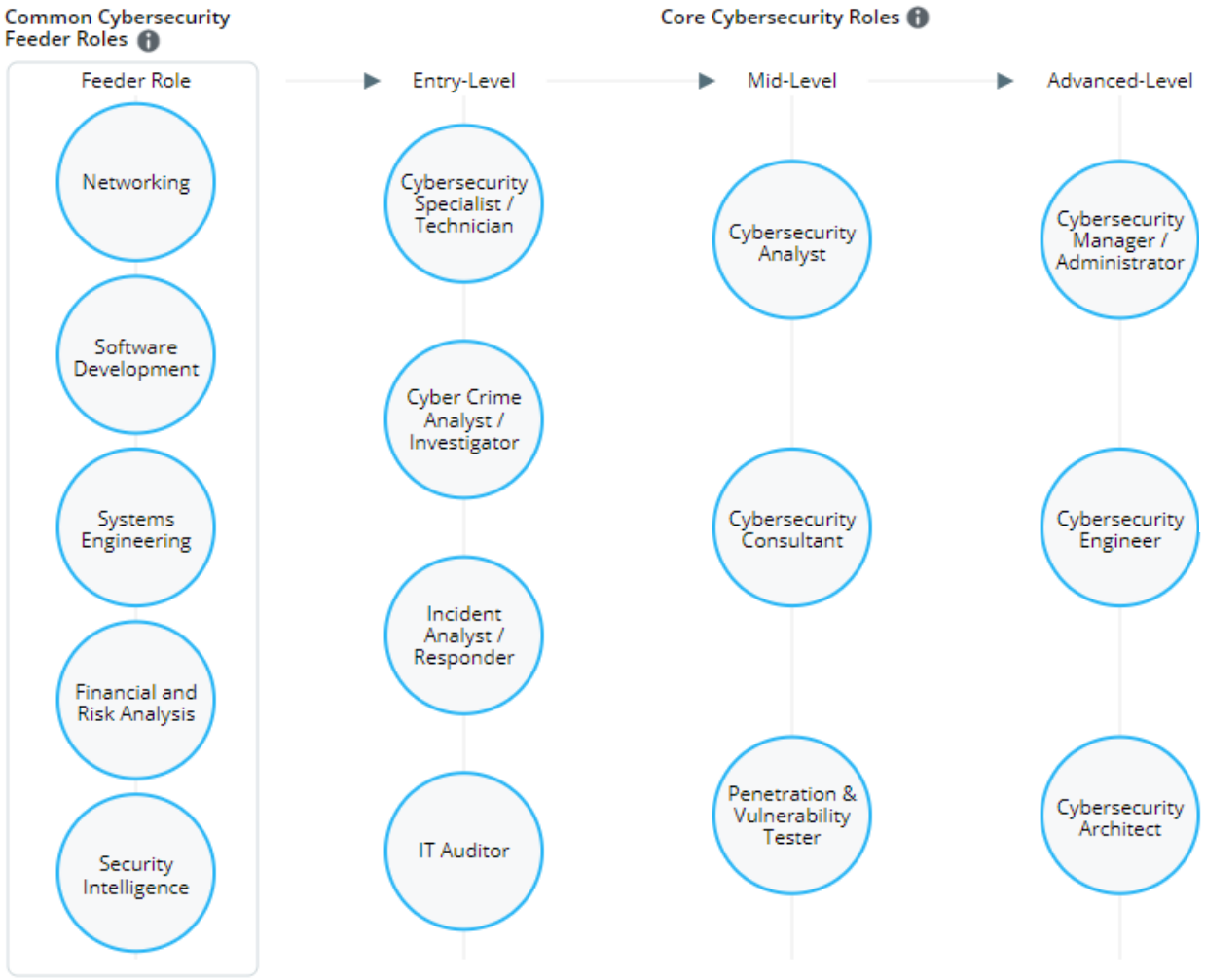
Algorithms

Behavioural Psychology

Identity and Access Management

Griffith UNIVERSITY
Queensland, Australia

How to become a cyber security professional?



Cybersecurity Engineer

AVERAGE SALARY
$108,000
Cybersecurity Engineer

COMMON JOB TITLES
- Security Engineer
- Network Security Engineer
- Information Security Engineer
- Senior Security Engineer
- Cyber Security Engineer

REQUESTED EDUCATION (%)

Sub-BA	Bachelor's Degree	Graduate Degree
11	67	23

TOP SKILLS REQUESTED
1. Information Security
2. Network Security
3. Linux
4. Information Systems
5. Python
6. Cryptography
7. Cisco
8. Project Management
9. Authentication

TOTAL JOB OPENINGS
40,988
Cybersecurity Engineer

COMMON NICE CYBERSECURITY WORKFORCE FRAMEWORK CATEGORIES
- Securely Provision
- Operate and Maintain
- Protect and Defend

TOP CERTIFICATIONS REQUESTED
- CISSP
- GIAC
- CISM
- CISA
- Security+

Penetration & Vulnerability Tester

AVERAGE SALARY
$102,000
Penetration & Vulnerability Tester

COMMON JOB TITLES
- Penetration Tester
- Application Security Architect
- Application Security Analyst
- Senior Penetration Tester
- Security Analyst III

REQUESTED EDUCATION (%)

Sub-BA	Bachelor's Degree	Graduate Degree
6	72	22

TOP SKILLS REQUESTED
1. Information Security
2. Penetration Testing
3. Linux
4. Vulnerability assessment
5. Python
6. Information Systems
7. Java
8. Open Web Application Security Project (OWASP)
9. Project Management

TOTAL JOB OPENINGS
9,826
Penetration & Vulnerability Tester

COMMON NICE CYBERSECURITY WORKFORCE FRAMEWORK CATEGORIES
- Analyze
- Protect and Defend

TOP CERTIFICATIONS REQUESTED
- GIAC
- CISA
- CISM
- GIAC Web Application Penetration Tester (GWAPT)
- Security+

https://www.cyberseek.org/pathway.html

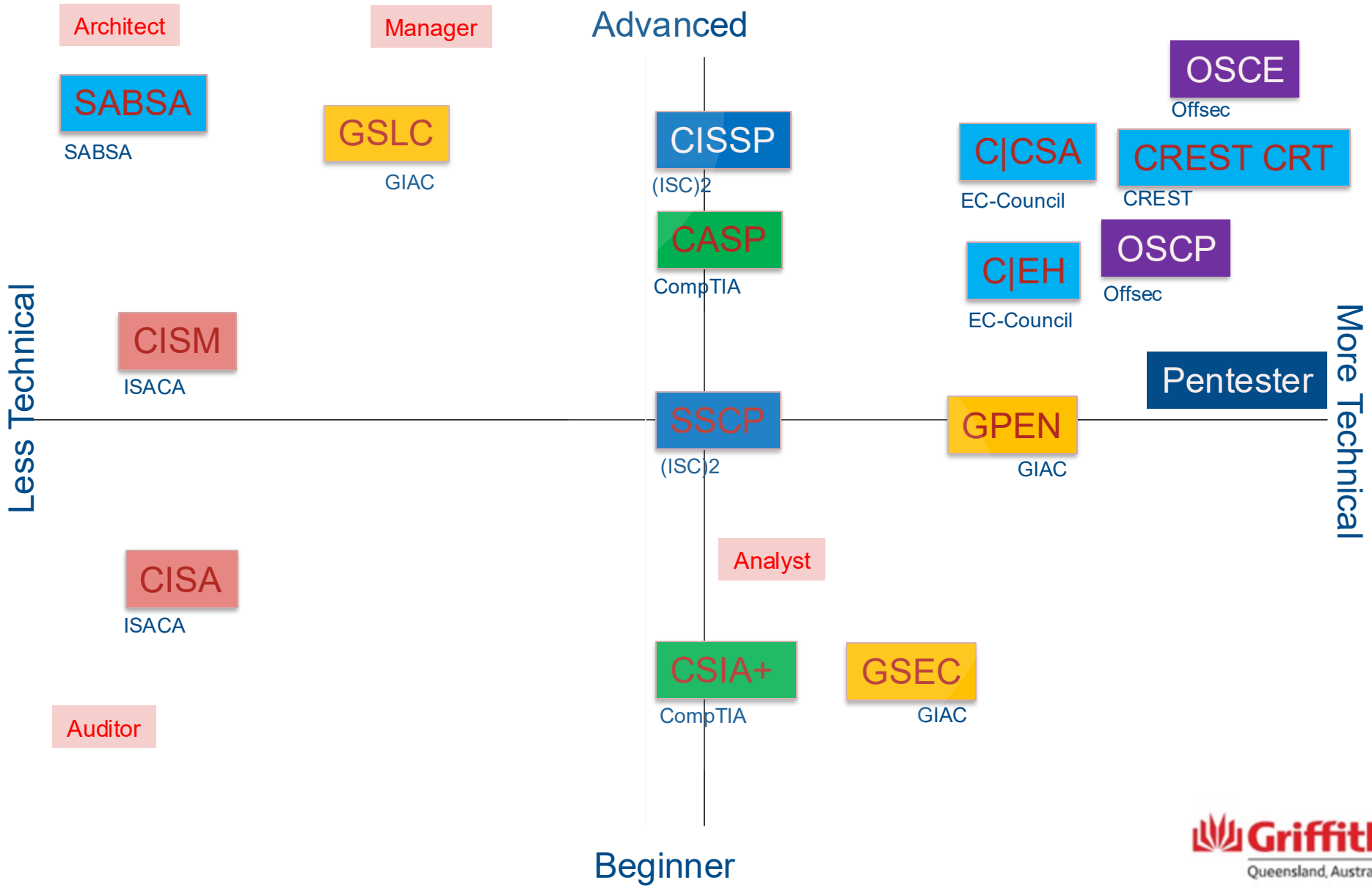
https://www.payscale.com/research/AU/Job=Information_Security_Specialist/Salary

How to become a cyber security professional?

V • T • E	Information security certifications	[hide]
CompTIA	Security+ *(S+)* • CySA+ *(formerly CSA+)* • CASP • PenTest+	
Cisco Systems	CCNA Security • CCNP Security • CCIE Security	
EC-Council	**CEH** • CNDA	
EITCI	EITCA/IS	
ISACA	CISA • CISM • CRISC	
(ISC)²	CISSP • SSCP • ISSMP • ISSEP • ISSAP	
Mile2	CPTE	
Offensive Security	OSCP • OSWP • OSCE • OSEE • OSWE	
eLearnSecurity	eCPPT	
GIAC	GISF • GSEC • GCIA • GCIH • GCUX • GCWN • GCED • GPEN • GWAPT • GAWN • GICSP • G7799 • GSNA • GISP • GSLC • GCPM • GSSP-JAVA • GSSP-.NET • GWEB • GCFE • GCFA • GREM • GNFA • GLEG • GSE	

https://en.wikipedia.org/wiki/Certified_Ethical_Hacker

Security Certifications



Griffith UNIVERSITY
Queensland, Australia

How to become a cyber security professional?

Popular Certifications:

- (ISC)2: CISSP – Certified Information System Security Professional
- CompTIA: CASP – CompTIA Advanced Security Practitioner
- ISACA:
  - CISA - Certified Information Systems Auditor
  - CISM - Certified Information Security Manager
- SANS/GIAC Certification
- Offensive Security:
  - OSCP – Offensive Security Certified Professional
  - OSCE – Offensive Security Certified Expert
- More:
  - Cryptography
  - Programming and algorithms
  - Networking and Routing(CCNA)

https://www.youtube.com/watch?v=Acqb1cdoVoM

Certifications (and a good CV) will only get you as far as the interview….

Griffith UNIVERSITY
Queensland, Australia

How to become a cyber security professional?

Career advice

- High demands in software developers who can write secure code
- Cybersecurity is a great career option, find a suitable pathway
- A multi-disciplinary area, CS and IT degrees provide solid foundation
- Plan your journey, **stay motivated and keep learning!**

https://www.bls.gov/careeroutlook/2018/interview/cybersecurity-consultant.htm?view_full

Summary

Module 1.1

1. Why is cybersecurity important?
2. Basics in Cybersecurity
3. Career advice

Next week: Module 1.2

Cyber Attacks