在網絡世界，要學懂知己知彼

Know the enemy and know yourself in Cyberspace

Mr. Frankie WONG, PISA

Agenda

- Intro to PISA and whoami
- Know your enemy in Cyberspace
- Know the Attack
- Know yourself
- How to build Cyber Defense
- Summary

Professional Information Security Association

About Us

PISA (專業資訊保安協會) is an independent and not-for-profit organization for information security professionals, with the primary objective of promoting information security awareness and best practice.

https://www.pisa.org.hk/

whoami

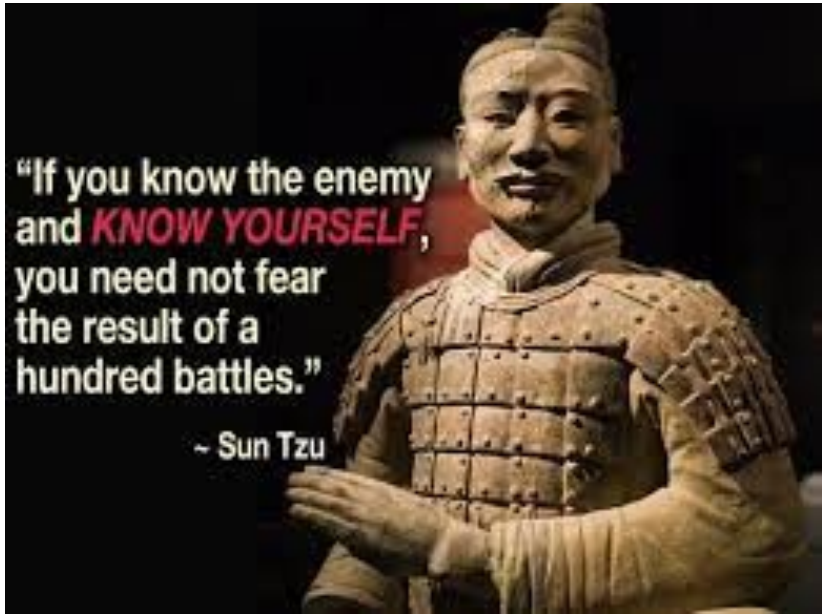
Mr. Frankie WONG

One of the Executive Committee members in PISA

10 years working experience in cybersecurity

Working for Security Operations and Cyber threat intelligence

Conducted sharing sessions on security topics



Know your enemy in Cyberspace

Know your enemy in Cyberspace

1. Cyber Criminals
    - Targets
    - Weapons
    - Aims: generating profits

2. Hacktivists
    - political agenda
    - religious belief
    - social ideology, etc.

Ref: https://www.javatpoint.com/types-of-cyber-attackers

Know your enemy in Cyberspace

3. State-sponsored Attacker
    - particular objectives
    - e.g. political, commercial or military interests

4. Insider Threats
    - Malicious
    - Accidental
    - Negligent

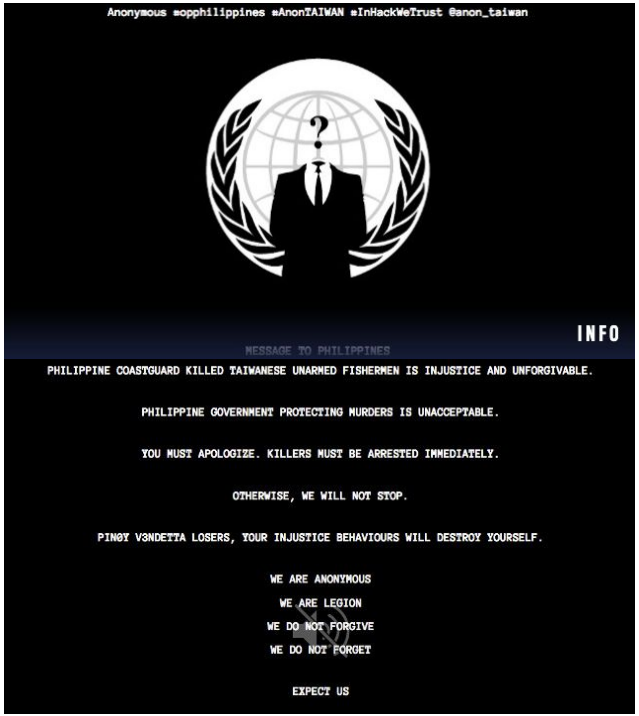
Ref: https://www.javatpoint.com/types-of-cyber-attackers

Exercise 1-1

Web Defacement

What kind of the enemy?

a. Criminals
b. Hacktivists
c. Insider Threats



Ref: https://www.rappler.com/nation/hackers-deface-philippine-government-sites-taiwan

Exercise 1-1

Web Deface

What kind o

a. Crimi

b. Hack

c. Inside

Case: In 2013, A number of Philippine government websites appear to have been defaced by hackers connecting themselves to **hacktivist group Anonymous**. A group called Anonymous Taiwan, which seems to use the newly-made @anon_taiwan Twitter handle, inserted new pages into the Department of Science and Technology (DOST) and Gov.ph websites.

Ref: https://www.rappler.com/nation/hackers-deface-philippine-government-sites-taiwan

Live Demo

Exercise 1-2

System crash / Data loss caused by departing employee

What kind of the enemy?

a. Criminals
b. State-sponsored Attacker
c. Insider Threats

Exercise 1-2

System crash / Data loss caused by departing employee

What kind of the enemy?

a. Criminals
b. State-sponsored Attacker
c. Insider Threats

Exercise 1-3

Ransomware Attack
- locked the files & ask for ransom

What kind of the enemy?

a. Criminals
b. State-sponsored Attacker
c. Insider Threats

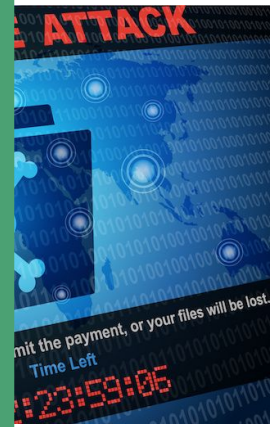
Exercise 1-3

Ransomwar
- locked the

What kind o

a. Crimi
b. State
c. Inside

Case: In 2017, WannaCry targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency. The US and UK governments have said North Korea was responsible for the WannaCry malware attack affecting hospitals, businesses and banks across the world.



Know the Attack

Know the Attack

2 main frameworks

- Cyber Kill Chain
  - The seven steps of the Cyber Kill Chain® enhance visibility into an attack and enrich an analyst’s understanding of an adversary’s tactics, techniques and procedures.
- Mitre ATT&CK
  - MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target.

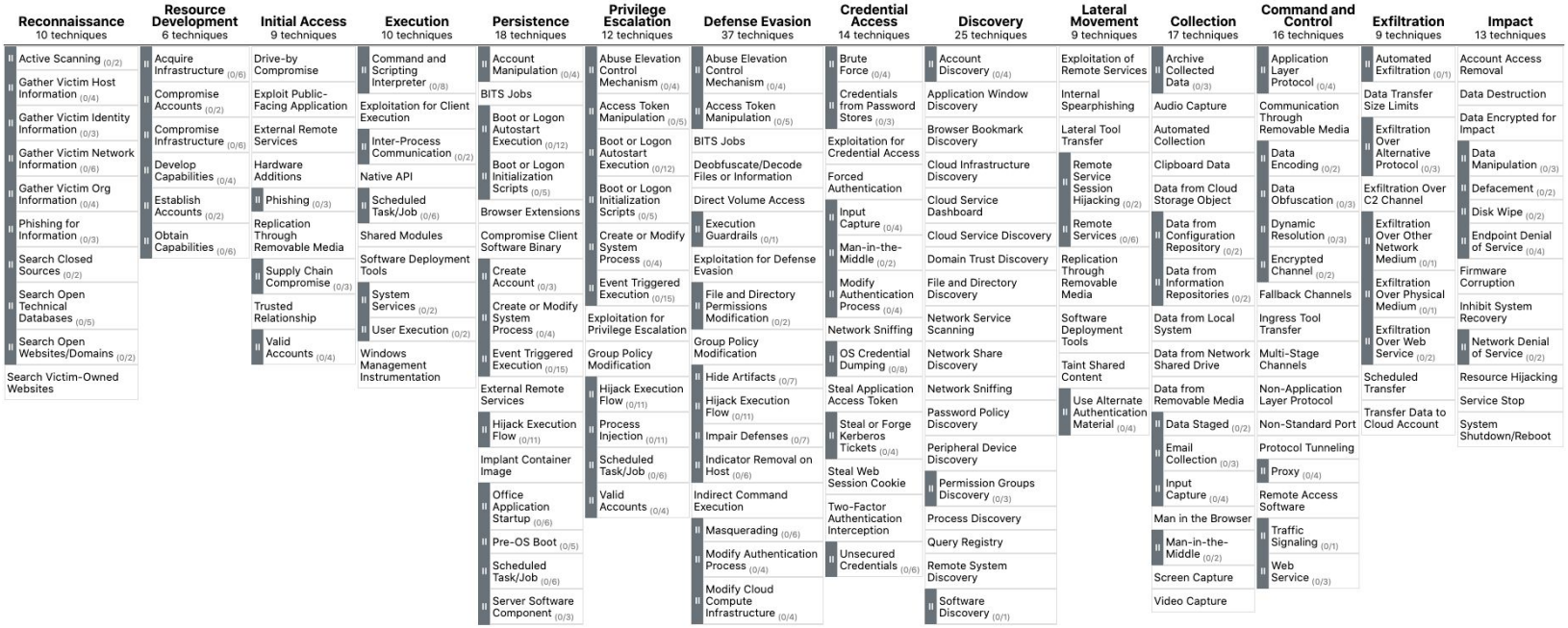
Ref: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
Ref: https://attack.mitre.org/

Know the Attack

Cyber Kill Chain

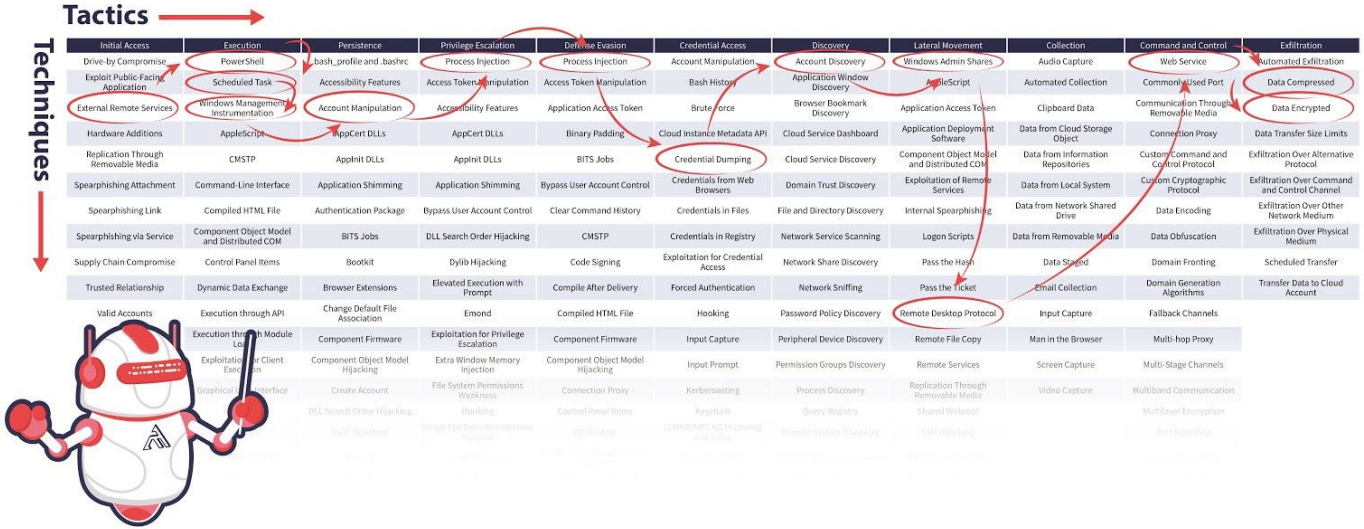
Know the Attack

Mitre ATT&CK



Know the Attack

Mitre ATT&CK



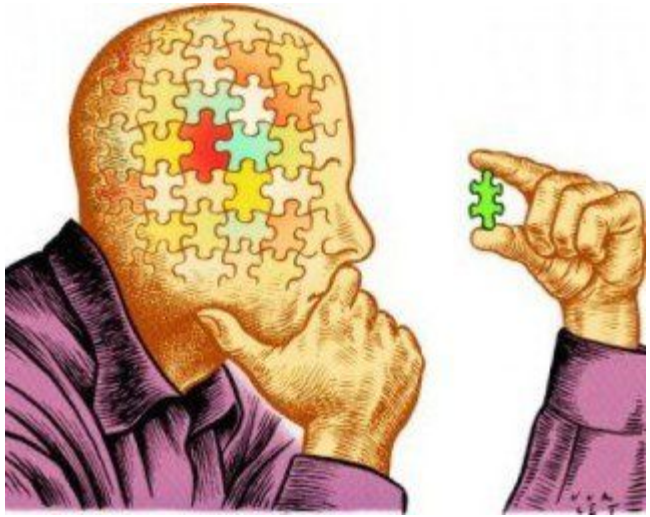
Ref: https://medium.com/cycraft/cycraft-classroom-mitre-att-ck-vs-cyber-kill-chain-vs-diamond-model-1cc8fa49a20f

Know yourself

Know yourself

We have to understand...

- Asset
  - Data? Critical Service?
- Risk / Threat
  - Visibility of the weakness?
- Controls
  - Fit the purpose? Effective?
- Mitigation
  - Any plan?
- Recovery / Compensation
  - Make sure business operating?



Know yourself

Do a simple self-check for your understanding...

HKCERT - Check Your Cyber Security Readiness

7 Habits of Cyber Security for SMEs

- Security Policy and Security Management
- Security Controls
  - Endpoint Security
  - Network Security
  - System Security
- Security Operations
  - Security Monitoring
  - Incident Handling
- User Awareness

https://www.hkcert.org/resources/check-your-cyber-security-readiness

How to build Cyber Defense

How to build Cyber Defense

No golden rule

Depends on your business and environment

2 main frameworks

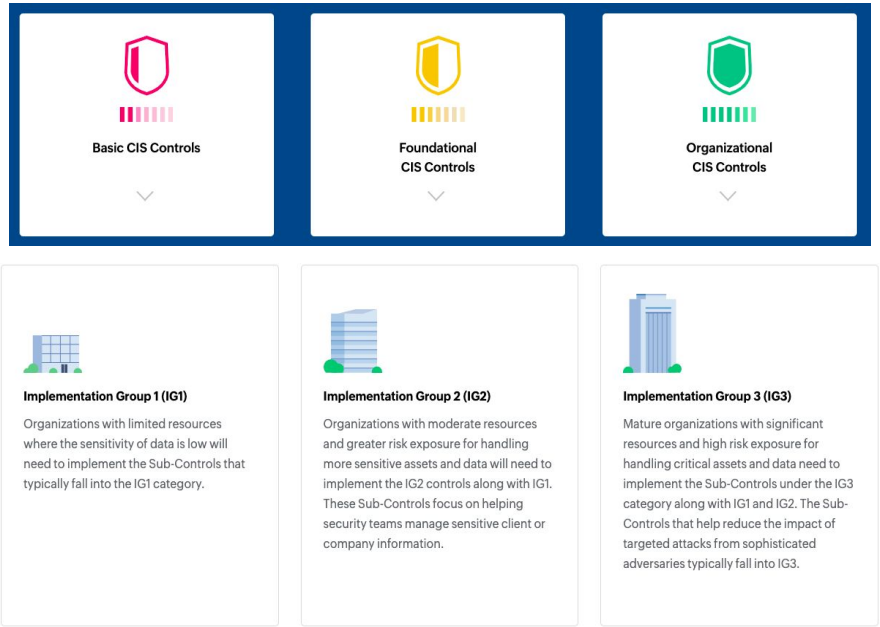
- CIS Controls
  - Developed by the Center for Internet Security®, the CIS Critical Security Controls are a prescriptive, prioritized set of cybersecurity best practices and defensive actions that can help prevent the most pervasive and dangerous attacks, and support compliance in a multi-framework era.
- NIST CSF
  - Created through collaboration between industry and government, the voluntary Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk.

Ref: https://www.cisecurity.org/controls/
Ref: https://www.nist.gov/cyberframework

How to build Cyber Defense

CIS Controls

- 18 controls
- Implementation Group 1 (IG1) is the definition of basic cyber hygiene and represents an emerging minimum standard of information security for all enterprises.
- An IG1 enterprise is small to medium-sized with limited IT and cybersecurity expertise to dedicate towards protecting IT assets and personnel.



Ref: https://www.cisecurity.org/controls/cis-controls-list/
Ref: https://www.manageengine.com/cis-critical-security-controls/index.html

How to build Cyber Defense

NIST CSF (Cyber Security Framework)

5 key functions - provide a comprehensive view of the lifecycle for managing cybersecurity over time.

- Identify
- Protect
- Detect
- Respond
- Recover

Ref: https://www.nist.gov/cyberframework/framework
Ref: https://csrc.nist.gov/Projects/cybersecurity-framework/nist-cybersecurity-framework-a-quick-start-guide

How to build Cyber Defense

NIST CSF (Cyber Security Framework)

- Not an enterprises?
- No problem. It has small business corner
  - https://www.nist.gov/itl/smallbusinesscyber
- [NISTIR 7621] - Small Business Information Security: The Fundamentals
  - It presents in non-technical language.
  - https://csrc.nist.gov/publications/detail/nistir/7621/rev-1/final

Ref: https://www.nist.gov/cyberframework/framework
Ref: https://csrc.nist.gov/Projects/cybersecurity-framework/nist-cybersecurity-framework-a-quick-start-guide

How to build Cyber Defense

[NISTIR 7621] - Small Business Information Security: The Fundamentals

3.1 IDENTIFY
- *Identify and control who has access to your business information*
- *Conduct Background Checks*
- *Require individual user accounts for each employee.*
- *Create policies and procedures for information security*

3.2 PROTECT
- *Limit employee access to data and information*
- *Install Surge Protectors and Uninterruptible Power Supplies (UPS)*
- *Patch your operating systems and applications*
- *Install and activate software and hardware firewalls on all your business networks*
- *Secure your wireless access point and networks*
- *Set up web and email filters*
- *Use encryption for sensitive business information*
- *Dispose of old computers and media safely*
- *Train your employees*

3.3 DETECT
- *Install and update anti-virus, -spyware, and other –malware programs*
- *Maintain and monitor logs*

3.4 RESPOND
- *Develop a plan for disasters and information security incidents*

3.5 RECOVER
- *Make full backups of important business data/information*
- *Make incremental backups of important business data/information*
- *Consider cyber insurance*
- *Make improvements to processes / procedures / technologies*

Ref: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf

Summary

Summary

Cyber Hygiene

- Cyber hygiene refers to fundamental cybersecurity best practices that an organization's security practitioners and users can undertake.

Cybersecurity Defense

- Know the enemy, know yourself
- Protection ➜ Detection + Response & Recovery
- No total solution. Need continuous improvement.

Thank you

Frankie WONG (t.me/fankewong)