

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

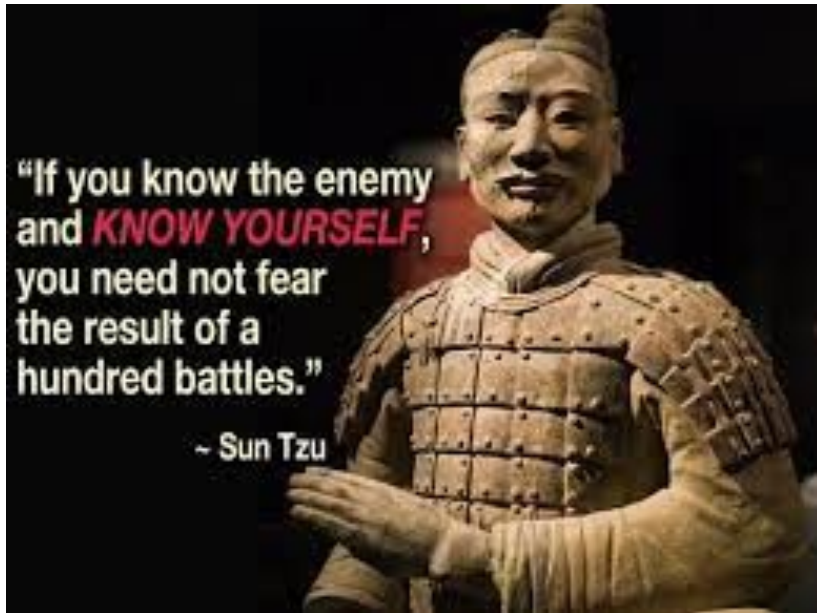
Mr. Frankie WONG

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.



# Know your enemy in Cyberspace

## 3. State-sponsored Attacker

- particular objectives
- e.g. political, commercial or military interests

## 4. Insider Threats

- Malicious
- Accidental
- Negligent

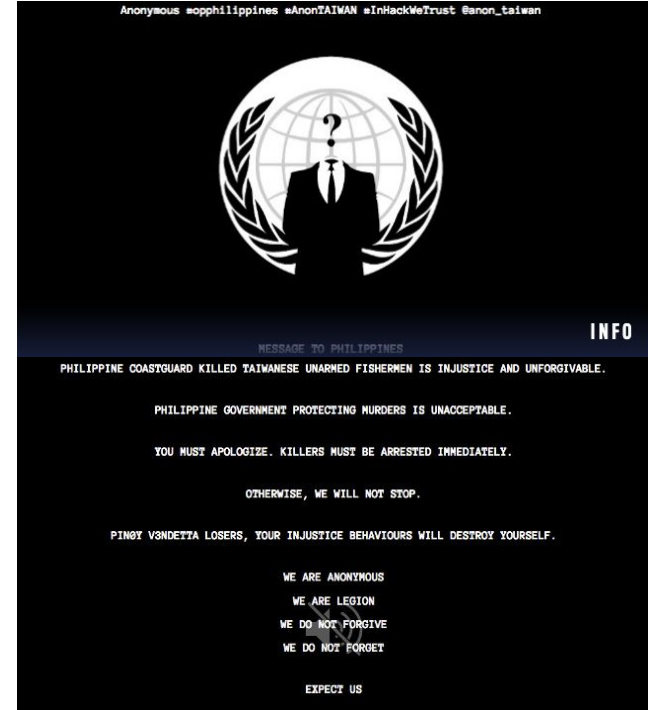


# Exercise 1-1

## Web Defacement

What kind of the enemy?

- a. Criminals
- b. Hacktivists
- c. Insider Threats





# Exercise 1-1

Web Defacement

What kind of

a. Criminal

b. Hacker

c. Insider

**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.



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

Ransomware

- locked the

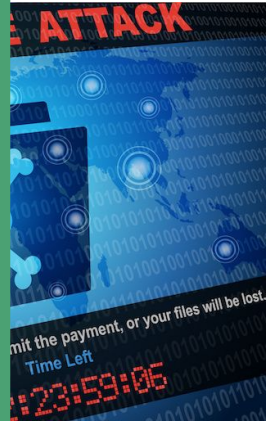
What kind of

a. Criminal

b. State

c. Insider

**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.



# Know the Attack

## Cyber Kill Chain



# Know the Attack

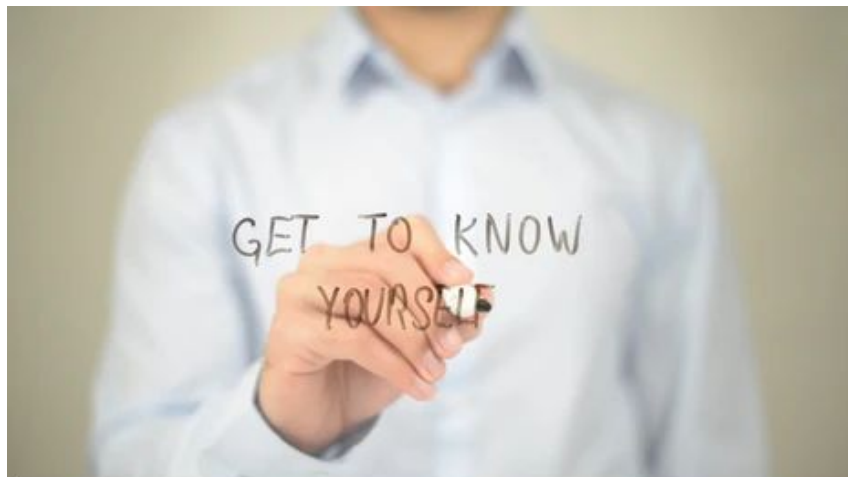
## Mitre ATT&CK

Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 14 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
<ul style="list-style-type: none"> <li>Active Scanning (0/2)</li> <li>Gather Victim Host Information (0/4)</li> <li>Gather Victim Identity Information (0/3)</li> <li>Gather Victim Network Information (0/6)</li> <li>Gather Victim Org Information (0/4)</li> <li>Phishing for Information (0/3)</li> <li>Search Closed Sources (0/2)</li> <li>Search Open Technical Databases (0/5)</li> <li>Search Open Websites/Domains (0/2)</li> <li>Search Victim-Owned Websites</li> </ul>	<ul style="list-style-type: none"> <li>Acquire Infrastructure (0/6)</li> <li>Compromise Accounts (0/2)</li> <li>Compromise Infrastructure (0/6)</li> <li>Develop Capabilities (0/4)</li> <li>Establish Accounts (0/2)</li> <li>Obtain Capabilities (0/6)</li> </ul>	<ul style="list-style-type: none"> <li>Drive-by Compromise</li> <li>Exploit Public-Facing Application</li> <li>External Remote Services</li> <li>Hardware Additions</li> <li>Phishing (0/3)</li> <li>Replication Through Removable Media</li> <li>Supply Chain Compromise (0/3)</li> <li>Trusted Relationship</li> <li>Valid Accounts (0/4)</li> </ul>	<ul style="list-style-type: none"> <li>Command and Scripting Interpreter (0/8)</li> <li>Exploitation for Client Execution</li> <li>Inter-Process Communication (0/2)</li> <li>Native API</li> <li>Scheduled Task/Job (0/6)</li> <li>Shared Modules</li> <li>Software Deployment Tools</li> <li>System Services (0/2)</li> <li>User Execution (0/2)</li> <li>Windows Management Instrumentation</li> </ul>	<ul style="list-style-type: none"> <li>Account Manipulation (0/4)</li> <li>BITS Jobs</li> <li>Boot or Logon Autostart Execution (0/12)</li> <li>Boot or Logon Initialization Scripts (0/5)</li> <li>Browser Extensions</li> <li>Create Account (0/3)</li> <li>Create or Modify System Process (0/4)</li> <li>Event Triggered Execution (0/15)</li> <li>External Remote Services</li> <li>Hijack Execution Flow (0/11)</li> <li>Implant Container Image</li> <li>Office Application Startup (0/6)</li> <li>Pre-OS Boot (0/5)</li> <li>Scheduled Task/Job (0/6)</li> <li>Server Software Component (0/3)</li> </ul>	<ul style="list-style-type: none"> <li>Abuse Elevation Control Mechanism (0/4)</li> <li>Access Token Manipulation (0/5)</li> <li>Boot or Logon Autostart Execution (0/12)</li> <li>Boot or Logon Initialization Scripts (0/5)</li> <li>Create or Modify System Process (0/4)</li> <li>Event Triggered Execution (0/15)</li> <li>Group Policy Modification</li> <li>Hijack Execution Flow (0/11)</li> <li>Process Injection (0/11)</li> <li>Scheduled Task/Job (0/6)</li> <li>Valid Accounts (0/4)</li> <li>Masquerading (0/6)</li> <li>Modify Authentication Process (0/4)</li> <li>Modify Cloud Infrastructure (0/4)</li> </ul>	<ul style="list-style-type: none"> <li>Abuse Elevation Control Mechanism (0/4)</li> <li>Access Token Manipulation (0/5)</li> <li>BITS Jobs</li> <li>Deobfuscate/Decode Files or Information</li> <li>Direct Volume Access</li> <li>Execution Guardrails (0/1)</li> <li>Exploitation for Defense Evasion</li> <li>File and Directory Permissions Modification (0/2)</li> <li>Group Policy Modification</li> <li>Hide Artifacts (0/7)</li> <li>Hijack Execution Flow (0/11)</li> <li>Impair Defenses (0/7)</li> <li>Indicator Removal on Host (0/6)</li> <li>Indirect Command Execution</li> <li>Masquerading (0/6)</li> <li>Modify Authentication Process (0/4)</li> <li>Modify Cloud Infrastructure (0/4)</li> </ul>	<ul style="list-style-type: none"> <li>Brute Force (0/4)</li> <li>Credentials from Password Stores (0/3)</li> <li>Exploitation for Credential Access</li> <li>Forced Authentication</li> <li>Input Capture (0/4)</li> <li>Man-in-the-Middle (0/2)</li> <li>Modify Authentication Process (0/4)</li> <li>Network Sniffing</li> <li>OS Credential Dumping (0/8)</li> <li>Steal Application Access Token</li> <li>Steal or Forge Kerberos Tickets (0/4)</li> <li>Steal Web Session Cookie</li> <li>Two-Factor Authentication Interception</li> <li>Unsecured Credentials (0/6)</li> </ul>	<ul style="list-style-type: none"> <li>Account Discovery (0/4)</li> <li>Application Window Discovery</li> <li>Browser Bookmark Discovery</li> <li>Cloud Infrastructure Discovery</li> <li>Cloud Service Dashboard</li> <li>Cloud Service Discovery</li> <li>Domain Trust Discovery</li> <li>File and Directory Discovery</li> <li>Network Service Scanning</li> <li>Network Share Discovery</li> <li>Network Sniffing</li> <li>Password Policy Discovery</li> <li>Peripheral Device Discovery</li> <li>Permission Groups Discovery (0/3)</li> <li>Process Discovery</li> <li>Query Registry</li> <li>Remote System Discovery</li> <li>Software Discovery (0/1)</li> </ul>	<ul style="list-style-type: none"> <li>Exploitation of Remote Services</li> <li>Internal Spearphishing</li> <li>Lateral Tool Transfer</li> <li>Remote Session Hijacking (0/2)</li> <li>Remote Services (0/6)</li> <li>Replication Through Removable Media</li> <li>Software Deployment Tools</li> <li>Taint Shared Content</li> <li>Use Alternate Authentication Material (0/4)</li> </ul>	<ul style="list-style-type: none"> <li>Archive Collected Data (0/3)</li> <li>Audio Capture</li> <li>Automated Collection</li> <li>Clipboard Data</li> <li>Data from Cloud Storage Object</li> <li>Data from Configuration Repository (0/2)</li> <li>Data from Information Repositories (0/2)</li> <li>Data from Local System</li> <li>Data from Network Shared Drive</li> <li>Data from Removable Media</li> <li>Data Staged (0/2)</li> <li>Email Collection (0/3)</li> <li>Input Capture (0/4)</li> <li>Man in the Browser</li> <li>Man-in-the-Middle (0/2)</li> <li>Screen Capture</li> <li>Video Capture</li> </ul>	<ul style="list-style-type: none"> <li>Application Layer Protocol (0/4)</li> <li>Communication Through Removable Media</li> <li>Data Encoding (0/2)</li> <li>Data Obfuscation (0/3)</li> <li>Dynamic Resolution (0/3)</li> <li>Encrypted Channel (0/2)</li> <li>Fallback Channels</li> <li>Ingress Tool Transfer</li> <li>Multi-Stage Channels</li> <li>Non-Application Layer Protocol</li> <li>Non-Standard Port</li> <li>Proxy (0/4)</li> <li>Remote Access Software</li> <li>Traffic Signaling (0/1)</li> <li>Web Service (0/3)</li> </ul>	<ul style="list-style-type: none"> <li>Automated Exfiltration (0/1)</li> <li>Data Transfer Size Limits</li> <li>Exfiltration Over Alternative Protocol (0/3)</li> <li>Exfiltration Over C2 Channel</li> <li>Exfiltration Over Other Network Medium (0/1)</li> <li>Exfiltration Over Physical Medium (0/1)</li> <li>Exfiltration Over Web Service (0/2)</li> <li>Scheduled Transfer</li> <li>Transfer Data to Cloud Account</li> </ul>	<ul style="list-style-type: none"> <li>Account Access Removal</li> <li>Data Destruction</li> <li>Data Encrypted for Impact</li> <li>Data Manipulation (0/3)</li> <li>Defacement (0/2)</li> <li>Disk Wipe (0/2)</li> <li>Endpoint Denial of Service (0/4)</li> <li>Firmware Corruption</li> <li>Inhibit System Recovery</li> <li>Network Denial of Service (0/2)</li> <li>Resource Hijacking</li> <li>Service Stop</li> <li>System Shutdown/Reboot</li> </ul>

# Know the Attack

## Mitre ATT&CK





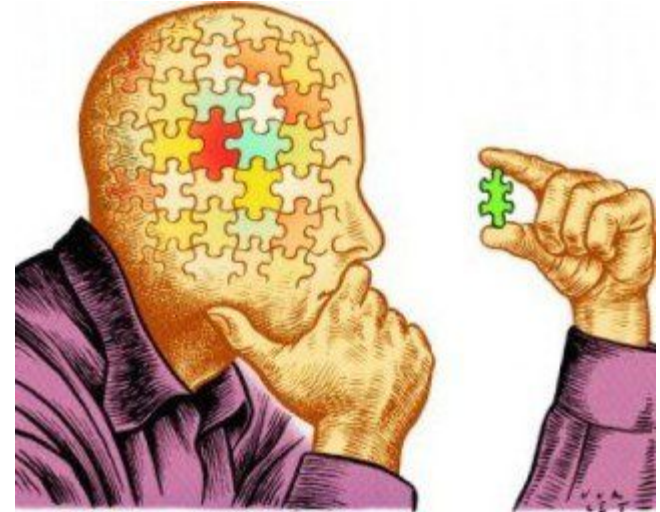
**Know yourself**

---

# 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/>

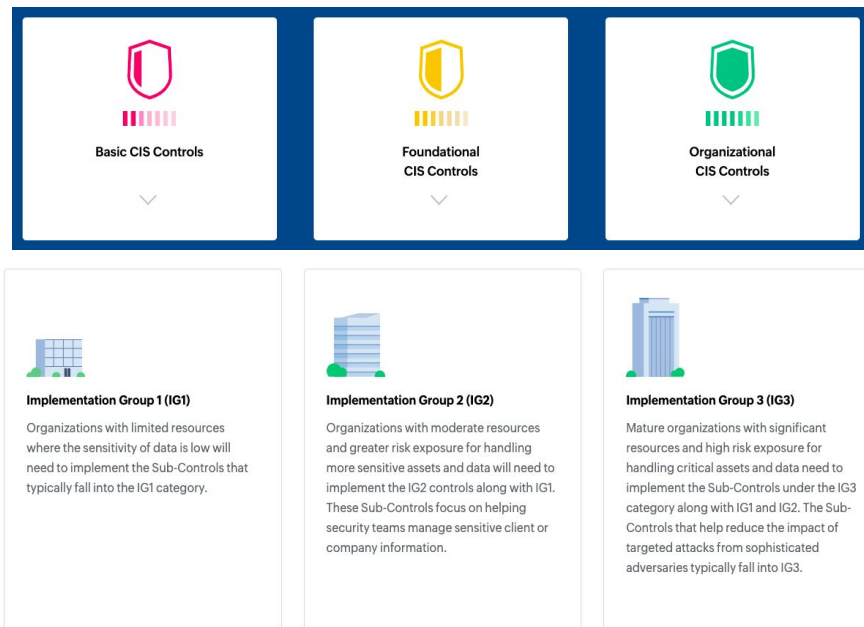
Ref: <https://www.nist.gov/cyberframework>



# 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.



# 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



# 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>



# 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 .....

## 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](https://t.me/fankewong))