The Seven Habits of Cyber Security for SMEs

S.C. Leung
Centre Manager
HKCERT

SMEs in Hong Kong

- Definition
  - < 100 staff (manufacturing)
  - < 50 staff (other sectors)

- ~ 338,000 SMEs

  (Source: TID, Dec 2018)

  - Over 98% of business establishments in Hong Kong and 46% employment in private sector

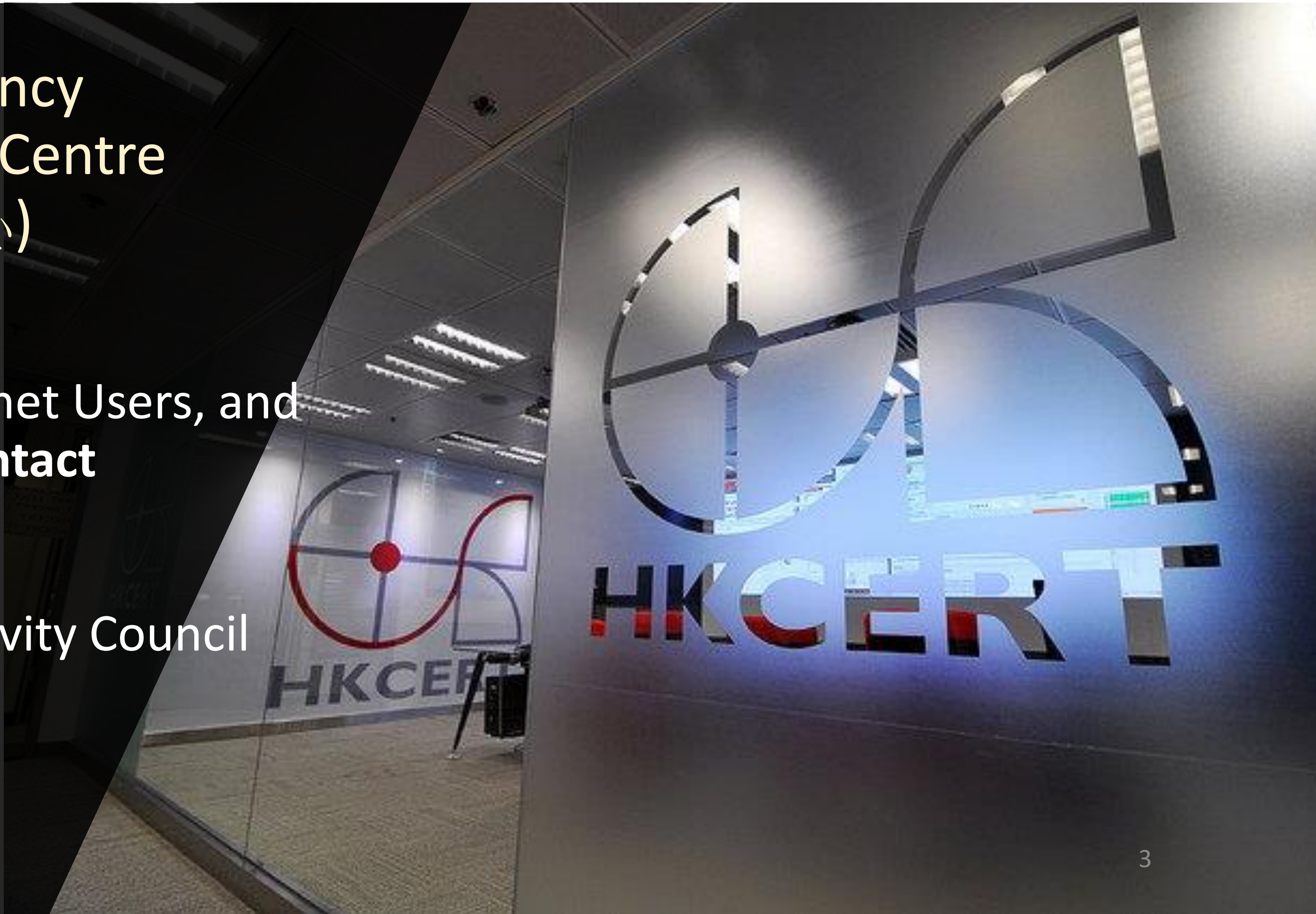
	Total number of SMEs @ Dec 2018	**338,113**
Services (97%)	Import/Export Trade and Wholesale	32%
	Professional and Business Services	15%
	Retail	13%
	Social and Personal Services	13%
	Financing and Insurance	8%
	Real Estate	5%
	Information and Communications	4%
	Accommodation and Food Services	4%
	Transportation, Storage, Courier Services	2%
Industry (3%)	Manufacturing	3%
	Mining; Electricity & Gas, Waste Mgmt; Construction	0.4%

HKCERT

Hong Kong Computer Emergency Response Team Coordination Centre (香港電腦保安事故協調中心)

- Established in 2001
- Serve local enterprises and Internet Users, and as the **international Point-of-Contact**

- Funded by Government
- Operated by Hong Kong Productivity Council



Services

- Incident Response **Free 24-hr Hotline**: 8105-6060

- Monitoring and Early Warning **Free subscription**

- Cross Border Coordination

- Awareness Promotion and Advices

Agenda

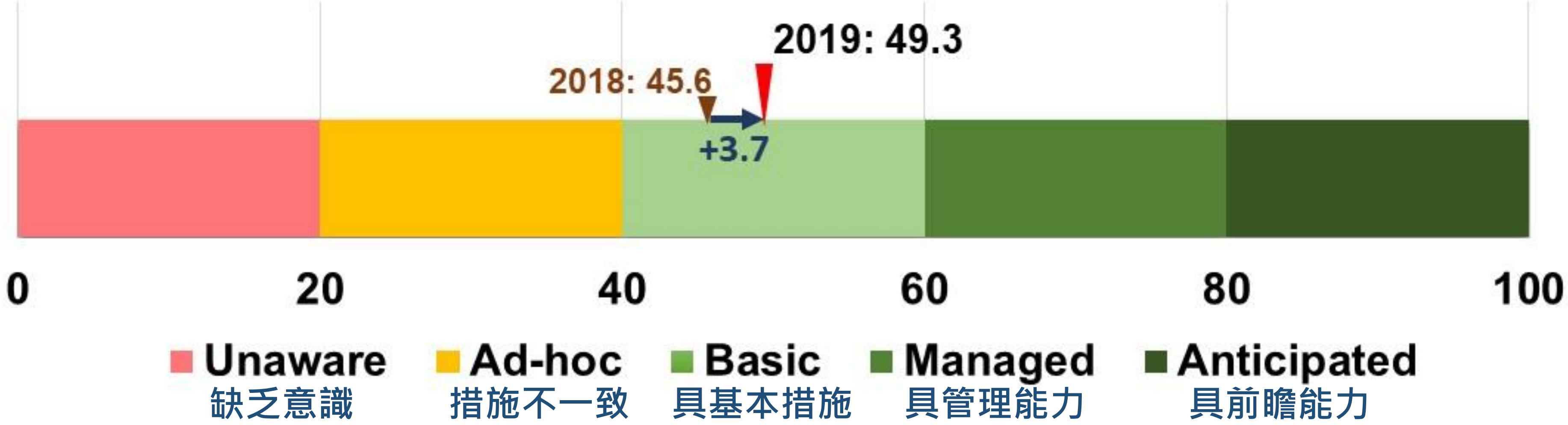
- Cyber Security Readiness of SMEs
- The “7 Habits of Cyber Security for SMEs” guideline
- Adapting the “7 Habits” in Your Environment

The SSH Hong Kong Enterprise Cyber Security Readiness Index 2019

SSH 香港企業網絡保安準備指數 2019

Overall Index at 49.3 (maximum being 100)

整體指數



Full Report: https://www.hkcert.org/my_url/en/blog/19041201

Source: HKPC

The SSH Hong Kong Enterprise Cyber Security Readiness Index 2019

SSH 香港企業網絡保安準備指數 2019

Components of Index

= **Enterprise Input (Readiness)** in four areas in past 12 months

SSH-HKECSRI

SSH 香港企業網絡保安準備指數

- Policy & Risk Assessment
  保安政策風險評估
- Technology Control
  技術控制
- Process Control
  流程控制
- Human Awareness
  員工意識

Source: HKPC

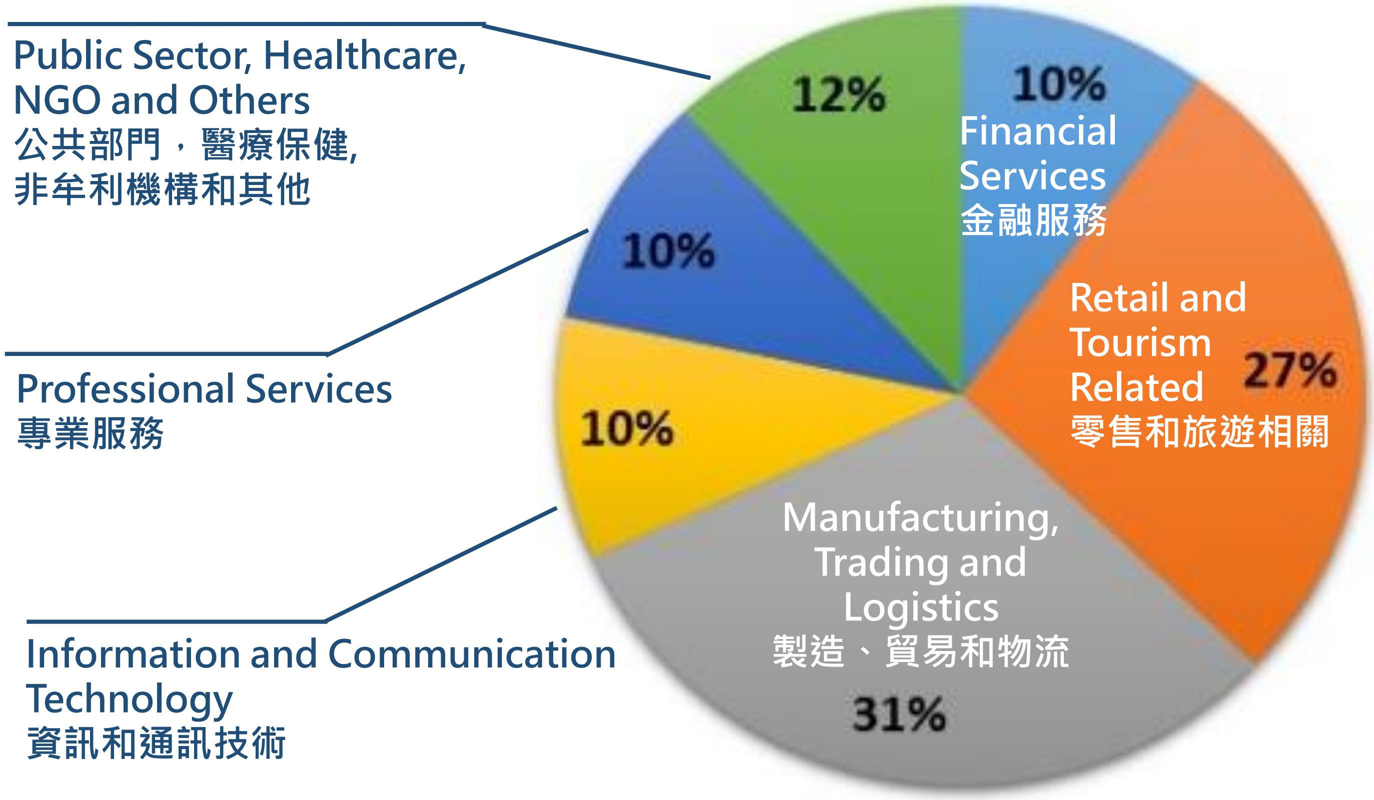
The SSH Hong Kong Enterprise Cyber Security Readiness Index 2019

SSH 香港企業網絡保安準備指數 2019

March 2019

54 Large Enterprises

296 SMEs

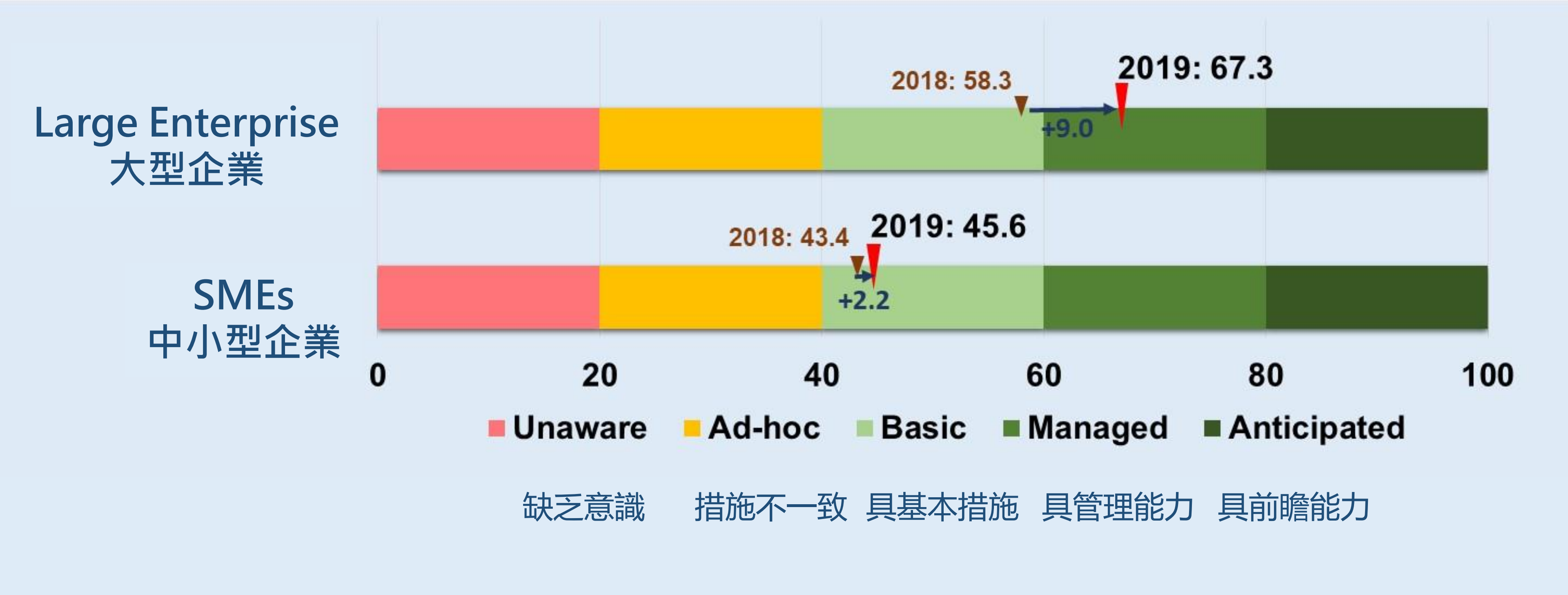


Source: HKPC

The SSH Hong Kong Enterprise Cyber Security Readiness Index 2019

SSH 香港企業網絡保安準備指數 2019

by Organisation Size



Source: HKPC

Enterprise Cyber Security Readiness Index by Business Category 按行業分類

	2019 Index 指數	2019 Level 級別
Financial Services 金融服務	66.0	Managed 具管理能力
Information and Communication Technology 資訊和通訊技術	55.8	Basic 具基本措施
Public sector, Healthcare NGO and Others 公共部門，醫療保健, 非牟利機構和其他	51.8	Basic 具基本措施
Professional Services 專業服務	48.0	Basic 具基本措施
Manufacturing, Trading and Logistics 製造，貿易和物流	45.8	Basic 具基本措施
Retail and Tourism related 零售和旅遊相關	44.0	Basic 具基本措施
All Business Categories 所有行業	49.3	Basic 具基本措施

Source: HKPC

The Seven Habits of Cyber Security for SMEs

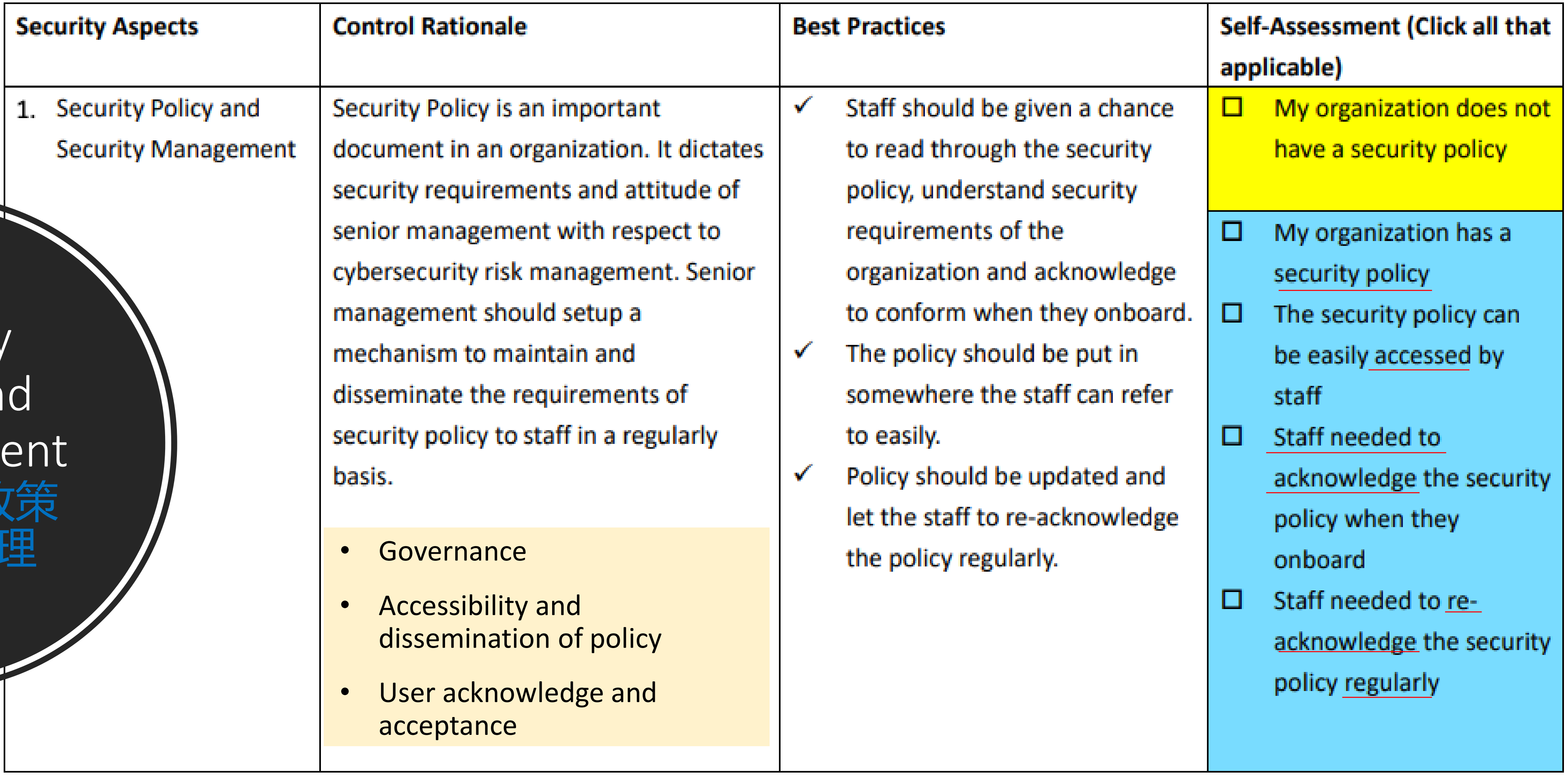
中小企網絡安全七大攻略

最佳實踐　　自我評估清單

1. Security Policy and Security Management
   資訊保安政策和資訊保安管理
2. Endpoint Security 端點保安
3. Network Security 網絡保安
4. System Security 系統保安
5. Security Monitoring 保安監察
6. Incident Handling 保安事故處理
7. User Awareness 用戶意識

https://www.hkcert.org/my_url/zh/guideline/18091101

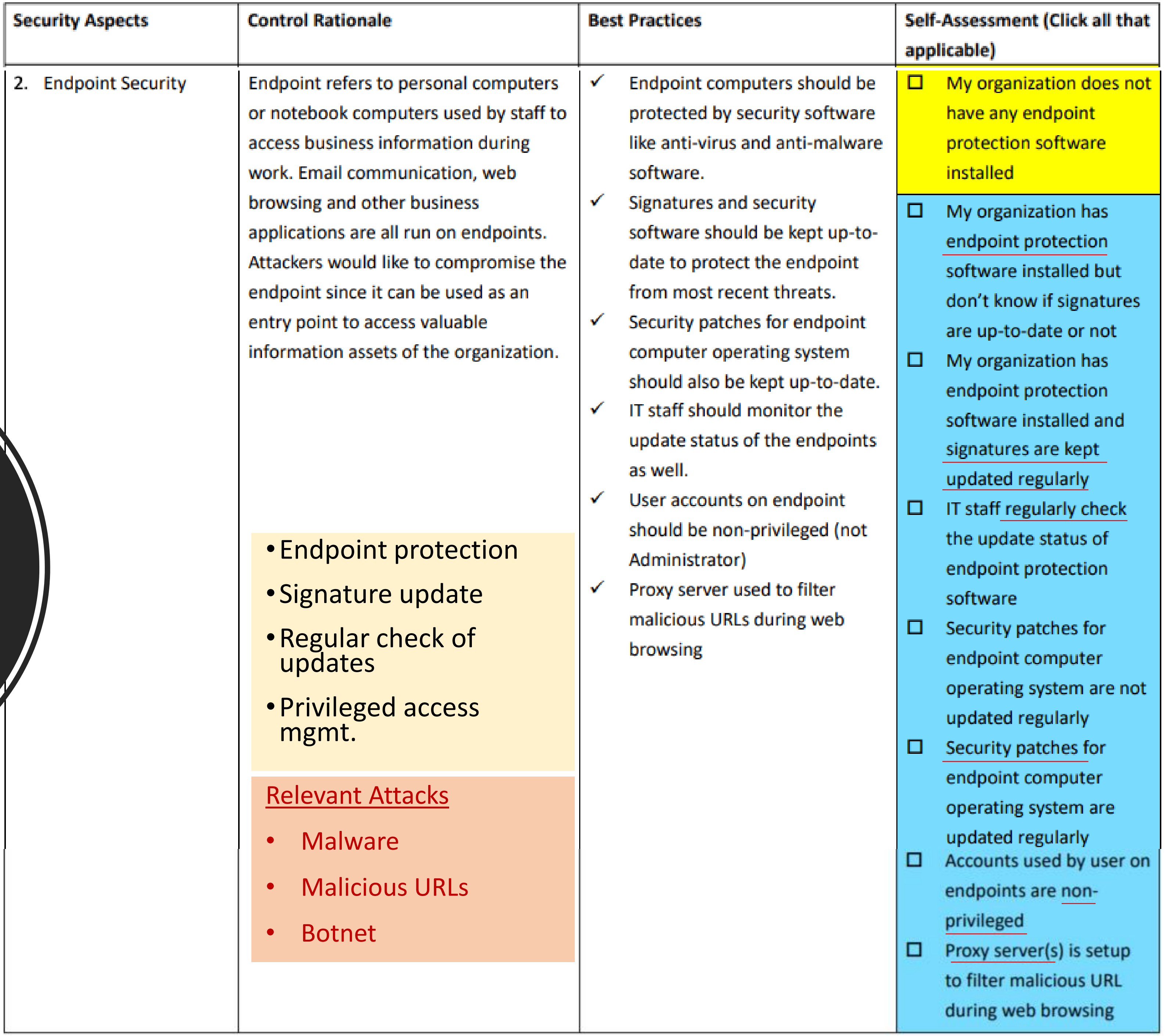
Security Policy and Management 資訊保安政策和保安管理



Security Aspects	Control Rationale	Best Practices	Self-Assessment (Click all that applicable)
1. Security Policy and Security Management	Security Policy is an important document in an organization. It dictates security requirements and attitude of senior management with respect to cybersecurity risk management. Senior management should setup a mechanism to maintain and disseminate the requirements of security policy to staff in a regularly basis.	✓ Staff should be given a chance to read through the security policy, understand security requirements of the organization and acknowledge to conform when they onboard. ✓ The policy should be put in somewhere the staff can refer to easily. ✓ Policy should be updated and let the staff to re-acknowledge the policy regularly.	☐ My organization does not have a security policy ☐ My organization has a security policy ☐ The security policy can be easily accessed by staff ☐ Staff needed to acknowledge the security policy when they onboard ☐ Staff needed to re-acknowledge the security policy regularly

- Governance
- Accessibility and dissemination of policy
- User acknowledge and acceptance

Endpoint Security
端點保安



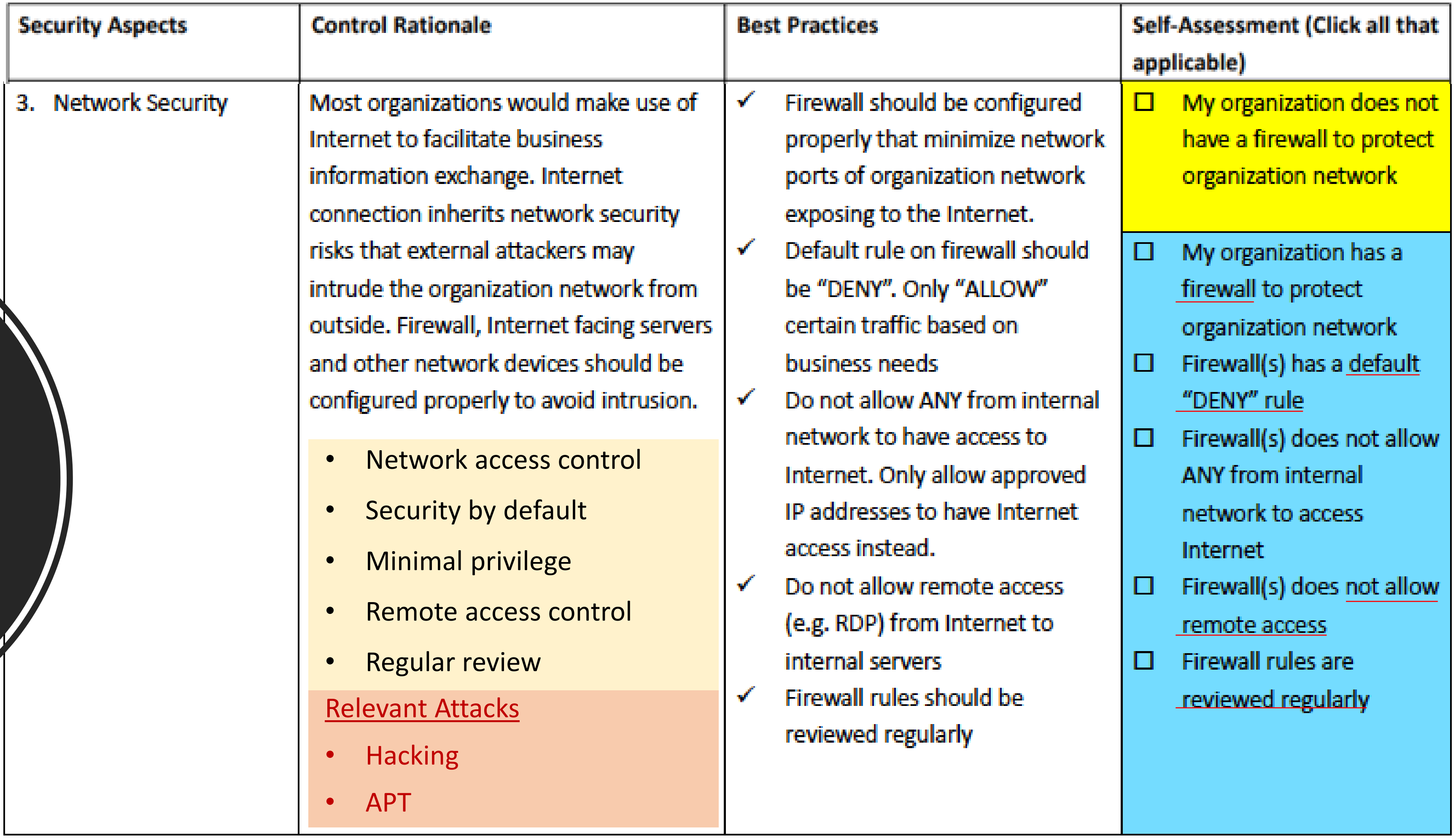
Security Aspects	Control Rationale	Best Practices	Self-Assessment (Click all that applicable)
2. Endpoint Security	Endpoint refers to personal computers or notebook computers used by staff to access business information during work. Email communication, web browsing and other business applications are all run on endpoints. Attackers would like to compromise the endpoint since it can be used as an entry point to access valuable information assets of the organization.	✓ Endpoint computers should be protected by security software like anti-virus and anti-malware software. ✓ Signatures and security software should be kept up-to-date to protect the endpoint from most recent threats. ✓ Security patches for endpoint computer operating system should also be kept up-to-date. ✓ IT staff should monitor the update status of the endpoints as well. ✓ User accounts on endpoint should be non-privileged (not Administrator) ✓ Proxy server used to filter malicious URLs during web browsing	☐ My organization does not have any endpoint protection software installed ☐ My organization has endpoint protection software installed but don't know if signatures are up-to-date or not ☐ My organization has endpoint protection software installed and signatures are kept updated regularly ☐ IT staff regularly check the update status of endpoint protection software ☐ Security patches for endpoint computer operating system are not updated regularly ☐ Security patches for endpoint computer operating system are updated regularly ☐ Accounts used by user on endpoints are non-privileged ☐ Proxy server(s) is setup to filter malicious URL during web browsing

- Endpoint protection
- Signature update
- Regular check of updates
- Privileged access mgmt.

Relevant Attacks

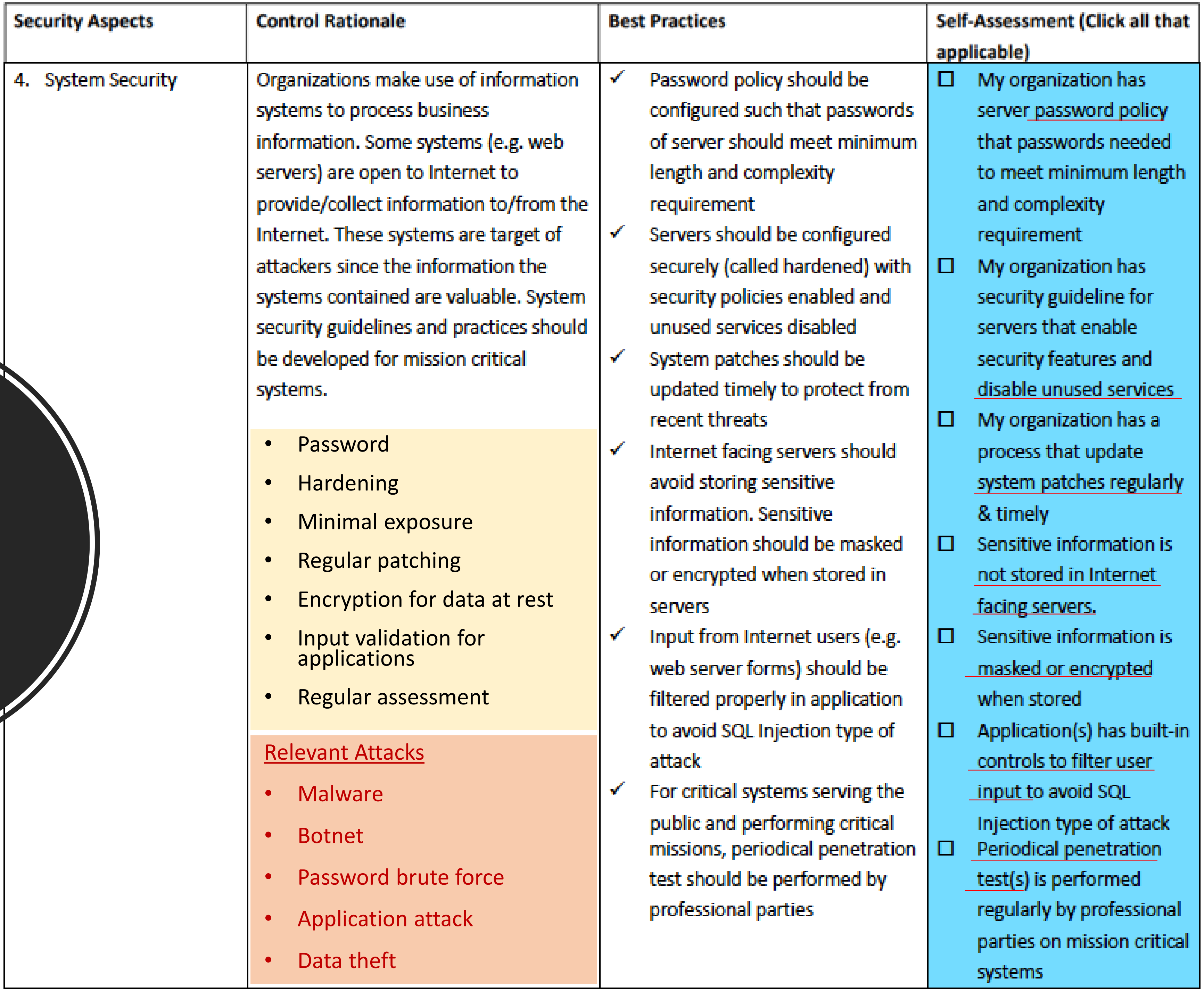
- Malware
- Malicious URLs
- Botnet

Network Security 網絡保安



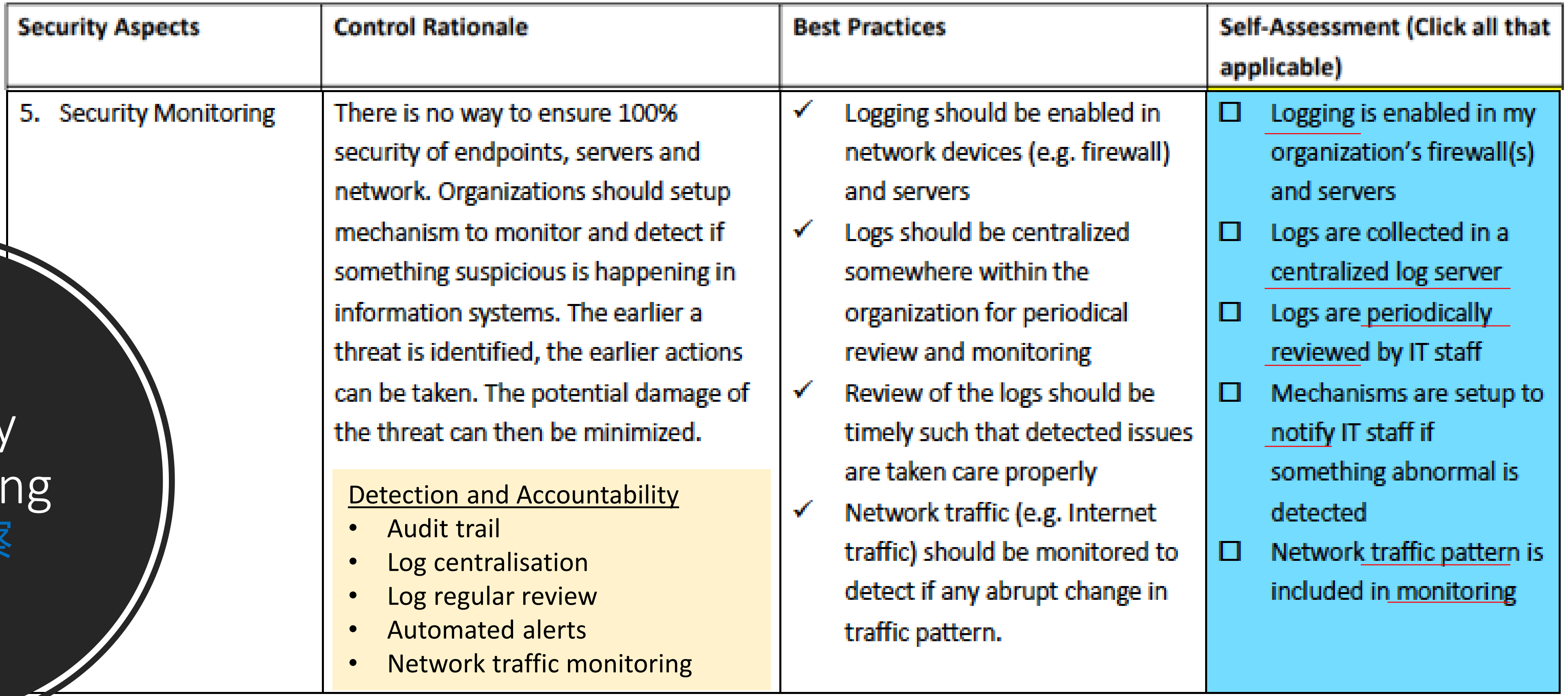
Security Aspects	Control Rationale	Best Practices	Self-Assessment (Click all that applicable)
3. Network Security	Most organizations would make use of Internet to facilitate business information exchange. Internet connection inherits network security risks that external attackers may intrude the organization network from outside. Firewall, Internet facing servers and other network devices should be configured properly to avoid intrusion. • Network access control • Security by default • Minimal privilege • Remote access control • Regular review Relevant Attacks • Hacking • APT	✓ Firewall should be configured properly that minimize network ports of organization network exposing to the Internet. ✓ Default rule on firewall should be "DENY". Only "ALLOW" certain traffic based on business needs ✓ Do not allow ANY from internal network to have access to Internet. Only allow approved IP addresses to have Internet access instead. ✓ Do not allow remote access (e.g. RDP) from Internet to internal servers ✓ Firewall rules should be reviewed regularly	□ My organization does not have a firewall to protect organization network □ My organization has a firewall to protect organization network □ Firewall(s) has a default "DENY" rule □ Firewall(s) does not allow ANY from internal network to access Internet □ Firewall(s) does not allow remote access □ Firewall rules are reviewed regularly

System Security
系統保安



Security Aspects	Control Rationale	Best Practices	Self-Assessment (Click all that applicable)
4. System Security	Organizations make use of information systems to process business information. Some systems (e.g. web servers) are open to Internet to provide/collect information to/from the Internet. These systems are target of attackers since the information the systems contained are valuable. System security guidelines and practices should be developed for mission critical systems. • Password • Hardening • Minimal exposure • Regular patching • Encryption for data at rest • Input validation for applications • Regular assessment Relevant Attacks • Malware • Botnet • Password brute force • Application attack • Data theft	✓ Password policy should be configured such that passwords of server should meet minimum length and complexity requirement ✓ Servers should be configured securely (called hardened) with security policies enabled and unused services disabled ✓ System patches should be updated timely to protect from recent threats ✓ Internet facing servers should avoid storing sensitive information. Sensitive information should be masked or encrypted when stored in servers ✓ Input from Internet users (e.g. web server forms) should be filtered properly in application to avoid SQL Injection type of attack ✓ For critical systems serving the public and performing critical missions, periodical penetration test should be performed by professional parties	□ My organization has server password policy that passwords needed to meet minimum length and complexity requirement □ My organization has security guideline for servers that enable security features and disable unused services □ My organization has a process that update system patches regularly & timely □ Sensitive information is not stored in Internet facing servers. □ Sensitive information is masked or encrypted when stored □ Application(s) has built-in controls to filter user input to avoid SQL Injection type of attack □ Periodical penetration test(s) is performed regularly by professional parties on mission critical systems

Security Monitoring
保安監察



Security Aspects	Control Rationale	Best Practices	Self-Assessment (Click all that applicable)
5. Security Monitoring	There is no way to ensure 100% security of endpoints, servers and network. Organizations should setup mechanism to monitor and detect if something suspicious is happening in information systems. The earlier a threat is identified, the earlier actions can be taken. The potential damage of the threat can then be minimized.	✓ Logging should be enabled in network devices (e.g. firewall) and servers ✓ Logs should be centralized somewhere within the organization for periodical review and monitoring ✓ Review of the logs should be timely such that detected issues are taken care properly ✓ Network traffic (e.g. Internet traffic) should be monitored to detect if any abrupt change in traffic pattern.	□ Logging is enabled in my organization's firewall(s) and servers □ Logs are collected in a centralized log server □ Logs are periodically reviewed by IT staff □ Mechanisms are setup to notify IT staff if something abnormal is detected □ Network traffic pattern is included in monitoring

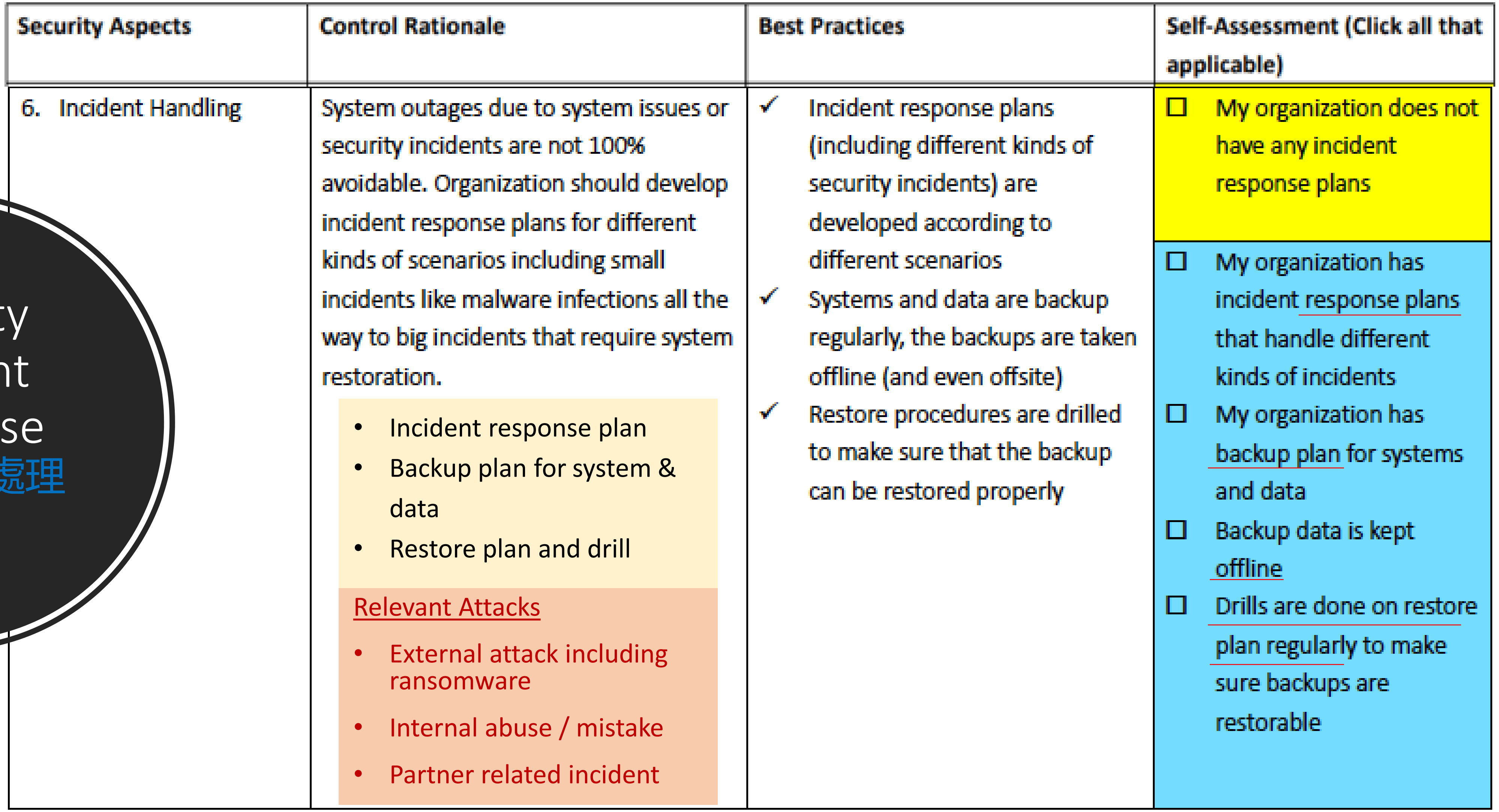
Detection and Accountability

- Audit trail
- Log centralisation
- Log regular review
- Automated alerts
- Network traffic monitoring

Relevant Attacks

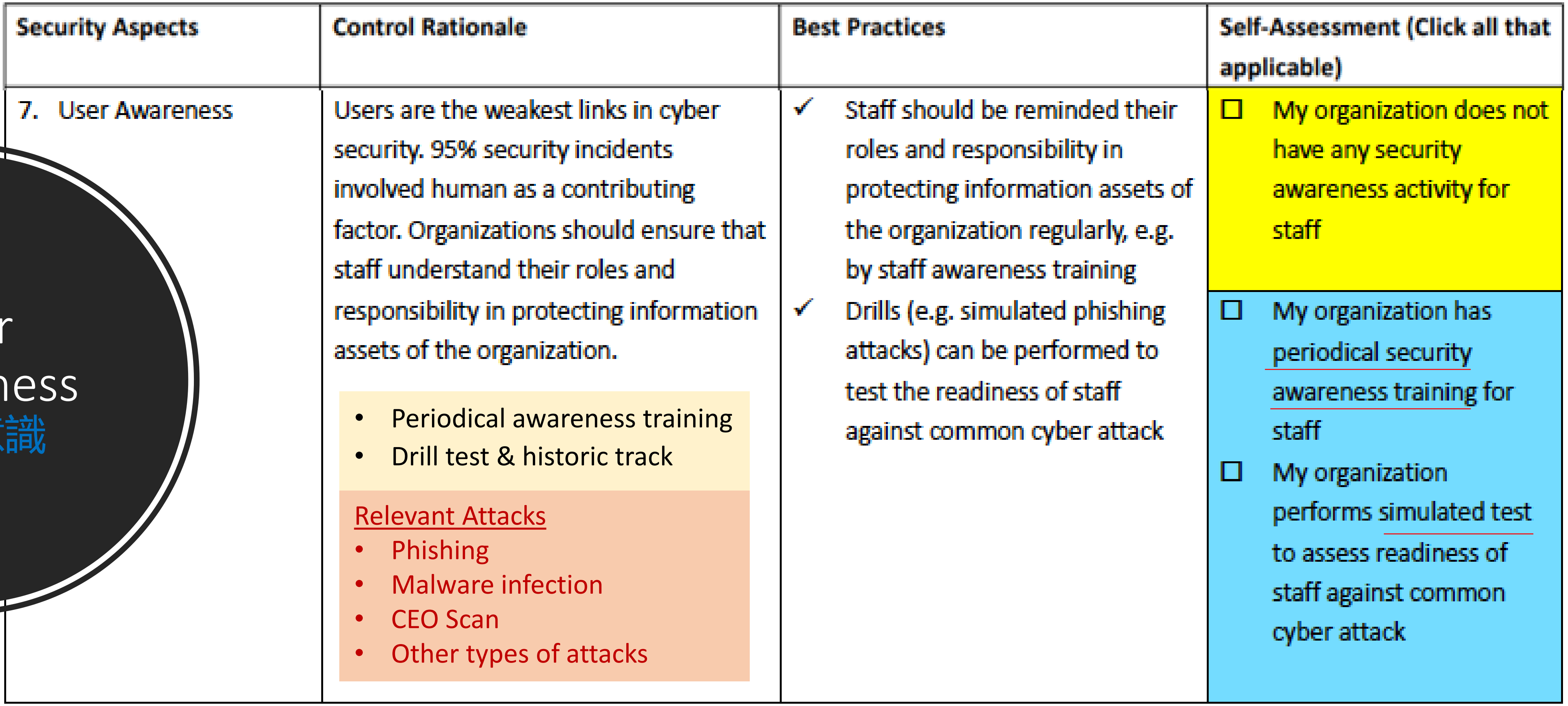
- External attack
- Compromised network including stealth ones
- Internal abuse / mistake
- All kinds of attacks

Security Incident Response
保安事故處理



Security Aspects	Control Rationale	Best Practices	Self-Assessment (Click all that applicable)
6. Incident Handling	System outages due to system issues or security incidents are not 100% avoidable. Organization should develop incident response plans for different kinds of scenarios including small incidents like malware infections all the way to big incidents that require system restoration. • Incident response plan • Backup plan for system & data • Restore plan and drill Relevant Attacks • External attack including ransomware • Internal abuse / mistake • Partner related incident	✓ Incident response plans (including different kinds of security incidents) are developed according to different scenarios ✓ Systems and data are backup regularly, the backups are taken offline (and even offsite) ✓ Restore procedures are drilled to make sure that the backup can be restored properly	□ My organization does not have any incident response plans □ My organization has incident response plans that handle different kinds of incidents □ My organization has backup plan for systems and data □ Backup data is kept offline □ Drills are done on restore plan regularly to make sure backups are restorable

User Awareness 用戶意識



Security Aspects	Control Rationale	Best Practices	Self-Assessment (Click all that applicable)
7. User Awareness	Users are the weakest links in cyber security. 95% security incidents involved human as a contributing factor. Organizations should ensure that staff understand their roles and responsibility in protecting information assets of the organization.	✓ Staff should be reminded their roles and responsibility in protecting information assets of the organization regularly, e.g. by staff awareness training ✓ Drills (e.g. simulated phishing attacks) can be performed to test the readiness of staff against common cyber attack	□ My organization does not have any security awareness activity for staff □ My organization has periodical security awareness training for staff □ My organization performs simulated test to assess readiness of staff against common cyber attack

- Periodical awareness training
- Drill test & historic track

Relevant Attacks

- Phishing
- Malware infection
- CEO Scan
- Other types of attacks

“7 Habits” guide applying to IoT systems

Endpoint

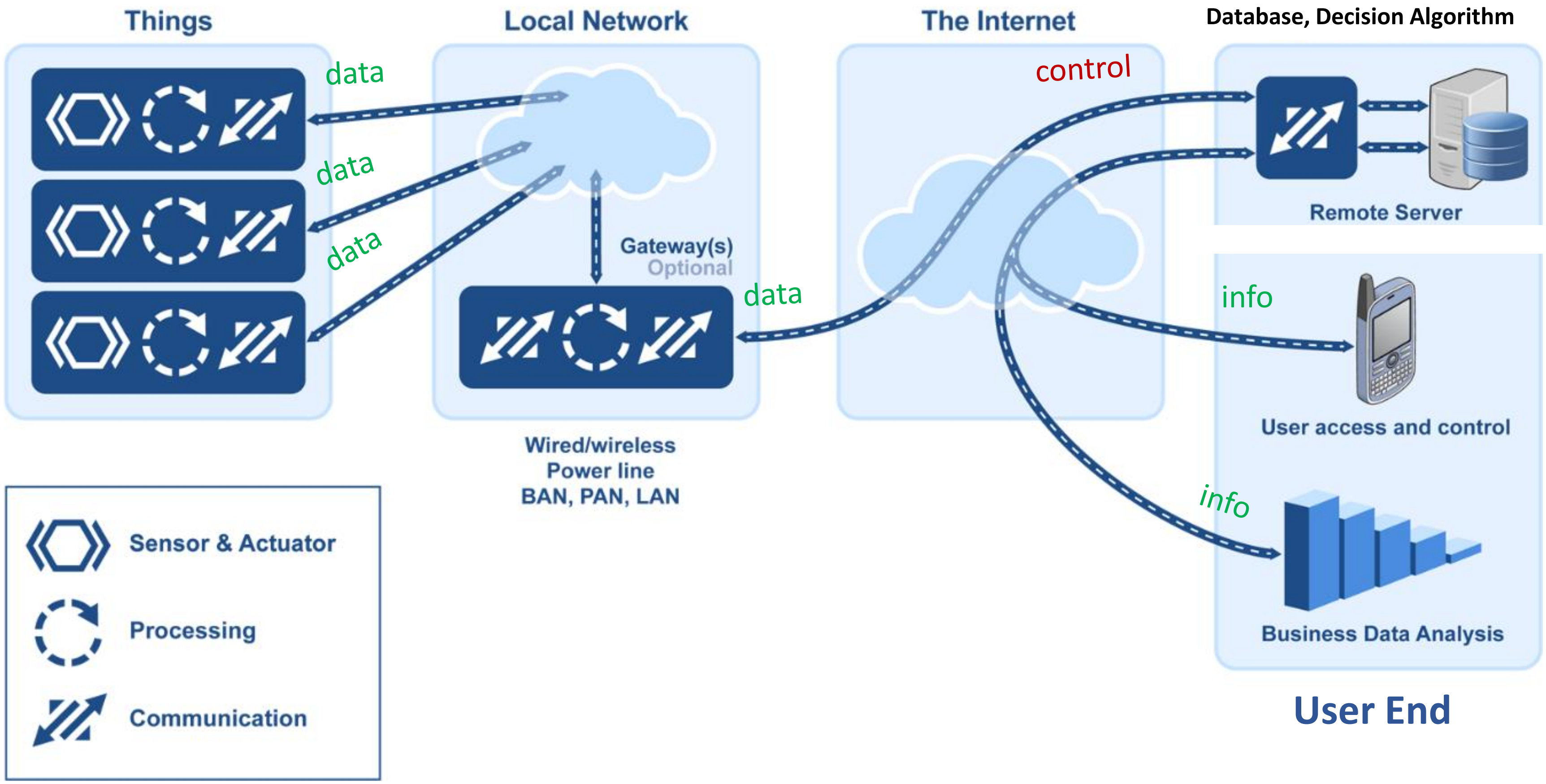
Sensor & Actuator

Network Monitoring

Infrastructure & Communication

System Monitoring

Platform & Backend



Decision Making

Endpoint

Information and Service

Image credit: http://micrium.com/designing-the-internet-of-things-part-1-iot-devices-and-local-networks

Self-assessment Score Calculation

- 33 Blue Box ✓,   5 Yellow Box ✓

- Score = number of Blue Box ✓ — number of Yellow Box ✓

-5至 2	3 至 10	11 至 18	19 至 25	26 至 33
Most Vulnerable	Vulnerable	Security to be strengthened	Adequate security	Robust and adequate security
保安十分鬆懈	保安鬆懈	保安須加強	保安充足	保安十分充足

The Seven Habits of Cyber Security for SMEs

Security Policy & Management
政策和管理

Endpoint Security
端點保安

Network Security
網絡保安

System Security
系統保安

Security Monitoring
保安監察

Incident Handling
保安事故處理

User Awareness
用戶意識

https://www.hkcert.org/my_url/zh/guideline/18091101

Adapting the "7 Habits" to Your Industry

- Identify your Critical Assets (data / systems)
- Identify the Threats and Attackers
- Assess the Risks
- Adapt Relevant Measures in the "7 Habits" Guide

Retail industry

Assets (System)

Point of Sale (POS)

Customer relationship management (CRM)

Assets (Data)

Credit card info.

Client info.

Threats

POS malware

POS bruteforce

Ransomware

Data Theft

Client account compromise

Attackers

Cyber criminals

Wi-fi guest users

7 Habits Measures

Policy: PCI-DSS compliance

Endpoint Security: keep updated version, monitor update status

Network Security: firewall, segregating client wifi from office network

System Security: change POS default password, password policy, patching

Monitoring: monitor POS log

Incident Response: data backup, offline backup copy, restore drill

Manufacturing industry

Assets (System)

Production management system

Database server

Assets (Data)

Intellectual properties (design, product ..)

Patents

Threats

Espionage

Data theft

Ransomware

Attacker

Cyber criminals

Business rivals

7 Habits Measures

Endpoint Security: keep updated version, monitor update status

Network Security: firewall, segregated factory and office networks

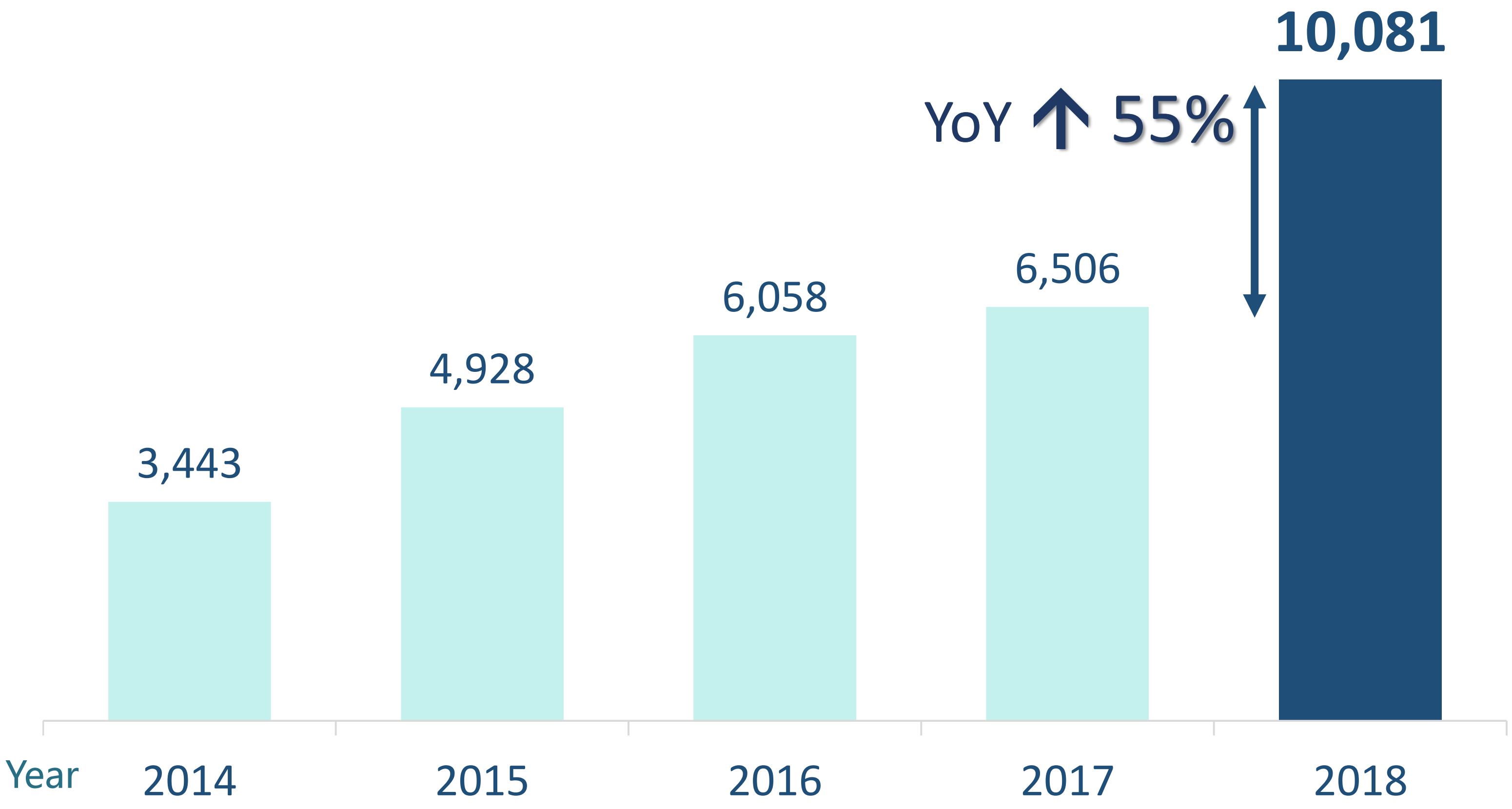
System Security: password policy, patch control systems, encrypt data (designs, patent documents)

Incident Response: data backup, offline backup copy, restore drill

User awareness: training, drill

Recent Attack Landscape

HKCERT Security Incident Report



Referred case contributed 95%

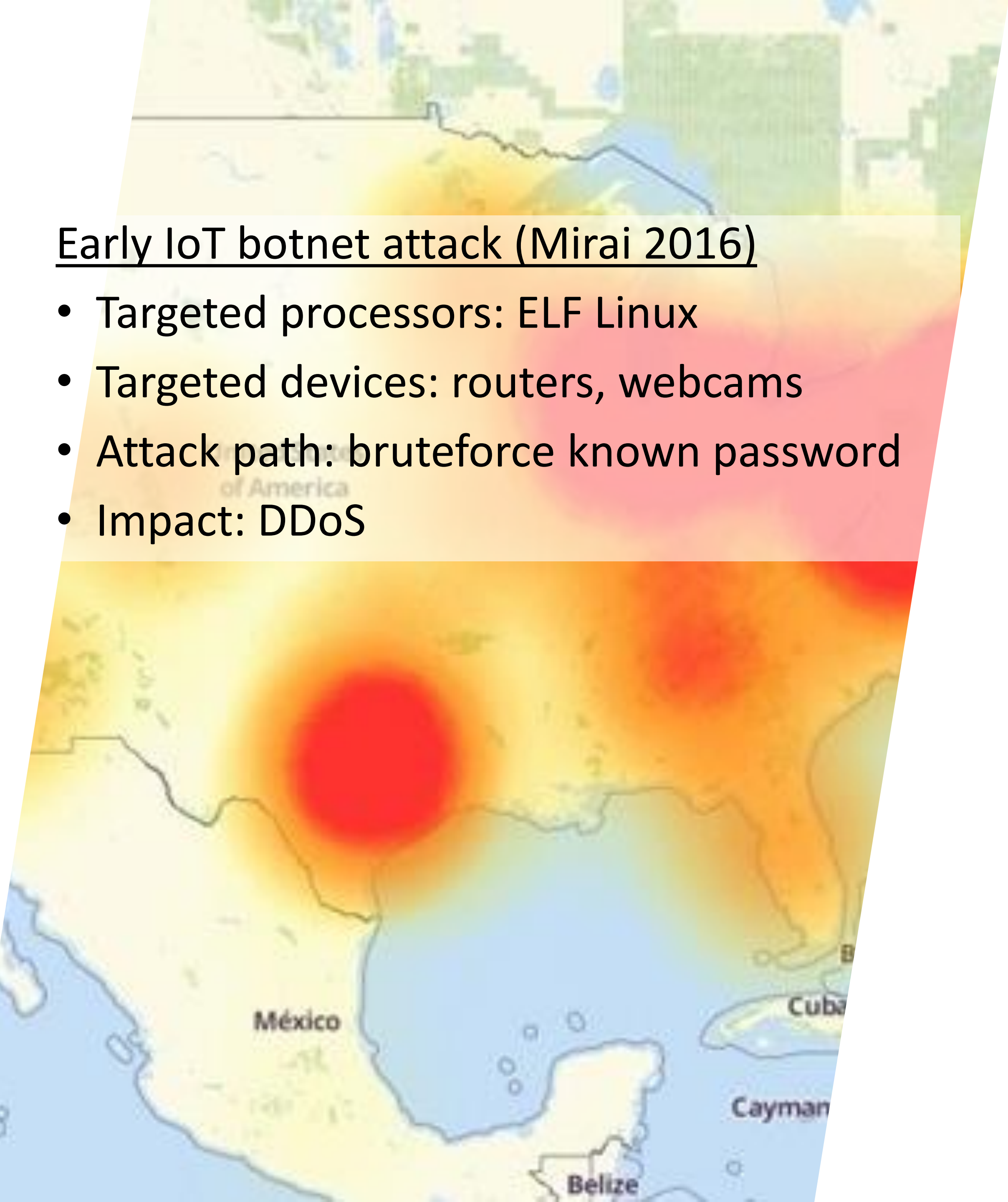
Source : HKCERT

Top Security Incidents according to HKCERT Statistics 2018

	2017	2018 (%)	YoY Variance 差異
Botnet 殭屍網絡	2,084	3,783 (37%)	+82%
Malware 惡意軟件	2,041	3,181 (32%)	+56%
Phishing 網絡釣魚	1,680	2,101 (21%)	+25%

Source : HKCERT

IoT botnet

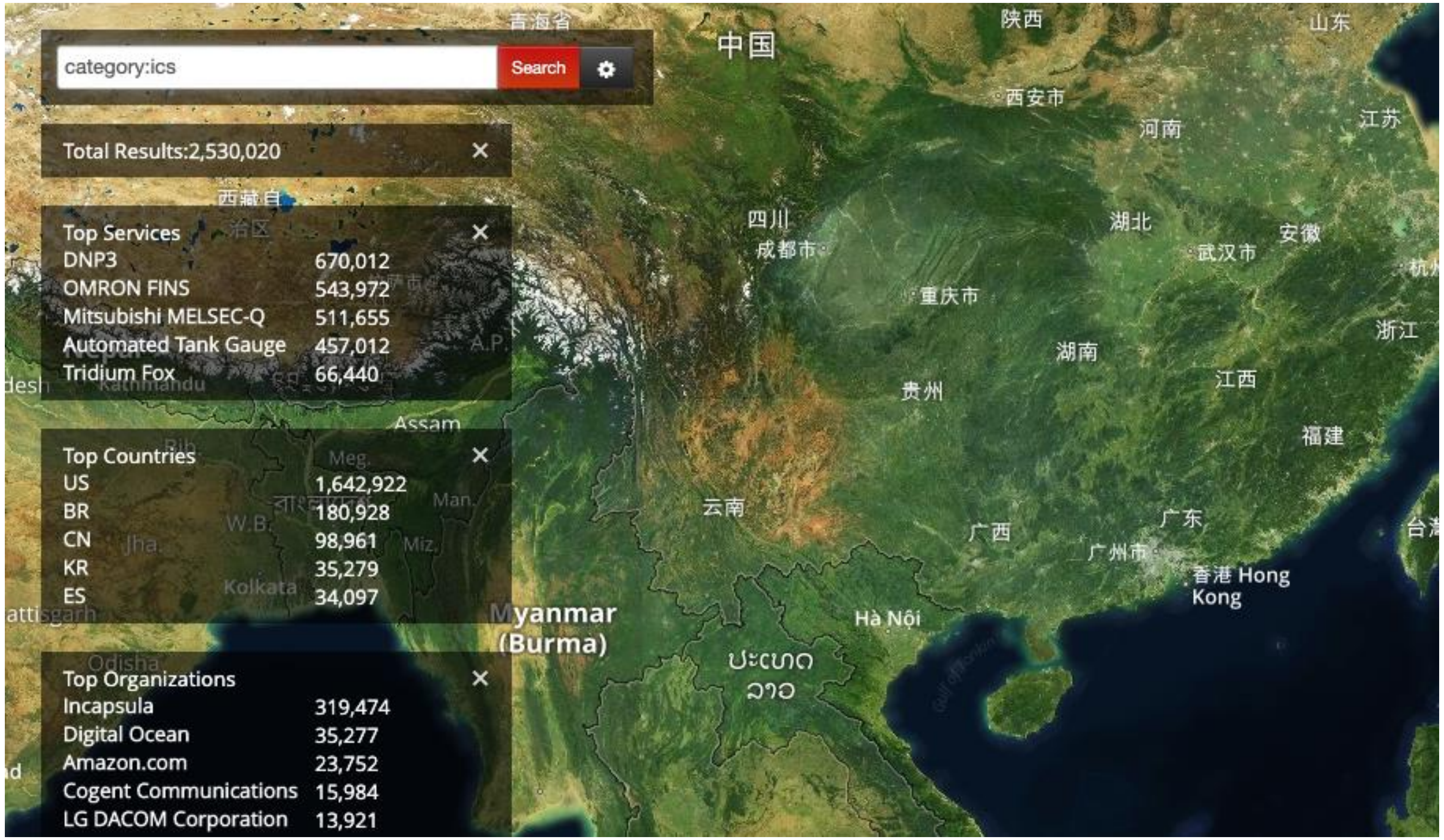


Early IoT botnet attack (Mirai 2016)

- Targeted processors: ELF Linux
- Targeted devices: routers, webcams
- Attack path: bruteforce known password
- Impact: DDoS

Recent development (2018-2019)

- **New Targeted Processors**
  - Altera Nios II, OpenRISC, Tensilica Xtensa, Xilinx MicroBlaze (Mirai)
- **New Targeted Devices**
  - ADB interface: Android based smartTV and home automation systems (ADB.Miner, HNS)
  - Modbus ICS (VPNFilter)
  - Network firewall (DoubleDoor)
- **New Attack Path**
  - Exploits (Double Door on Juniper : IoT Reaper (2017) on TR-069 RCE exploit of telecom routers
- **New features**
  - Cryptojacking: (Mirai, DriodMiner in 2017)
  - Exfiltration of sensitive data, modular architecture (Torii)
  - Modify DNS settings (VPNFilter, GhostDNS)



category:ics

Search

Total Results:2,530,020

Top Services	
DNP3	670,012
OMRON FINS	543,972
Mitsubishi MELSEC-Q	511,655
Automated Tank Gauge	457,012
Tridium Fox	66,440

Top Countries	
US	1,642,922
BR	180,928
CN	98,961
KR	35,279
ES	34,097

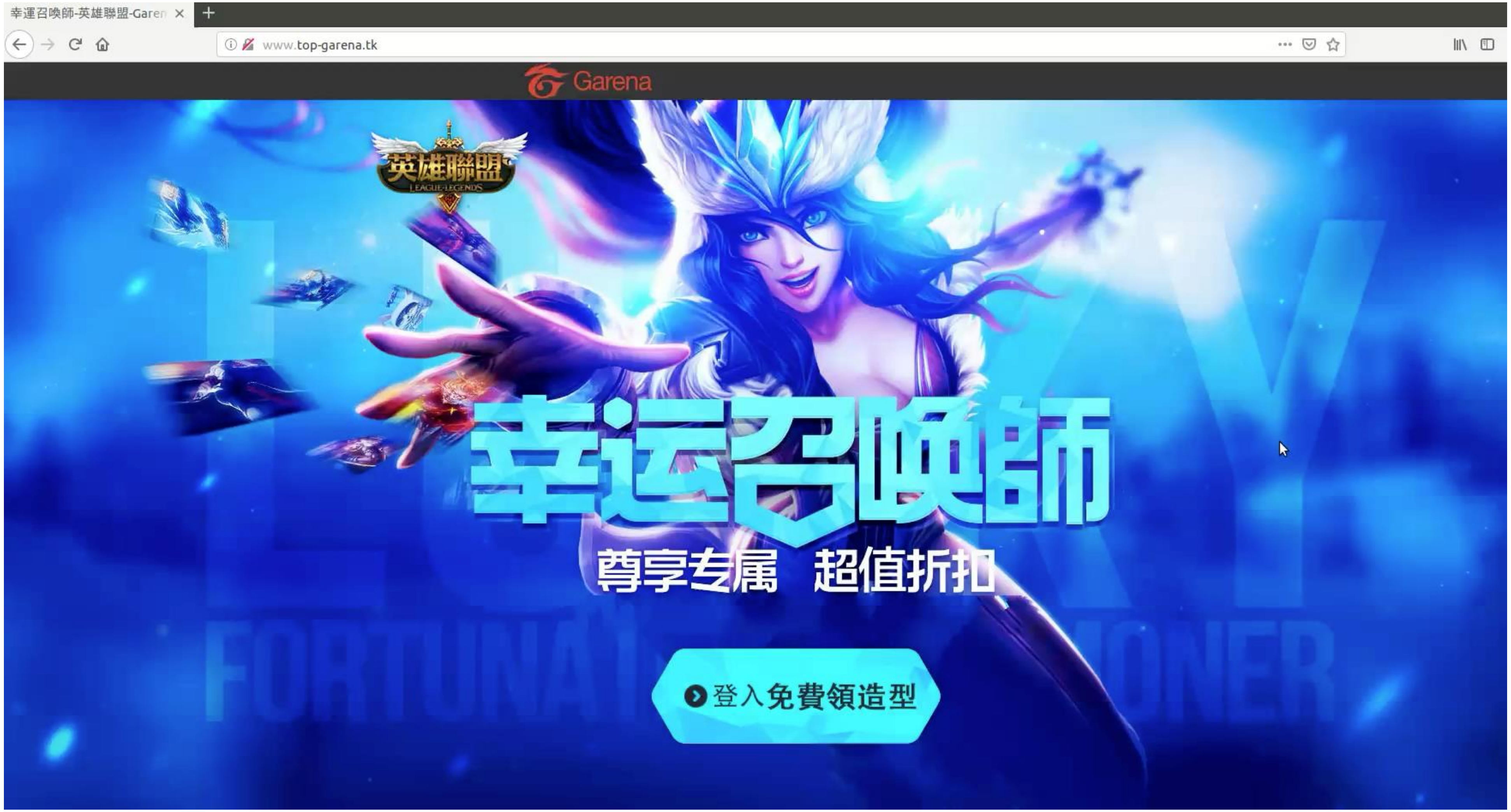
Top Organizations	
Incapsula	319,474
Digital Ocean	35,277
Amazon.com	23,752
Cogent Communications	15,984
LG DACOM Corporation	13,921

Beware:
Internet of Things exposed

- Internet device Search Engines keep on scanning for exposed devices

- Shodan Map
- **2,530,020** ICS components discovered as of May 2019

Phishing attack on the rise: online game as bait



Supply Chain Attack
– Video game development software (Apr 2019)

- 3 video game companies used corrupted version of Microsoft Visual Studio development tools in development created contaminated game software

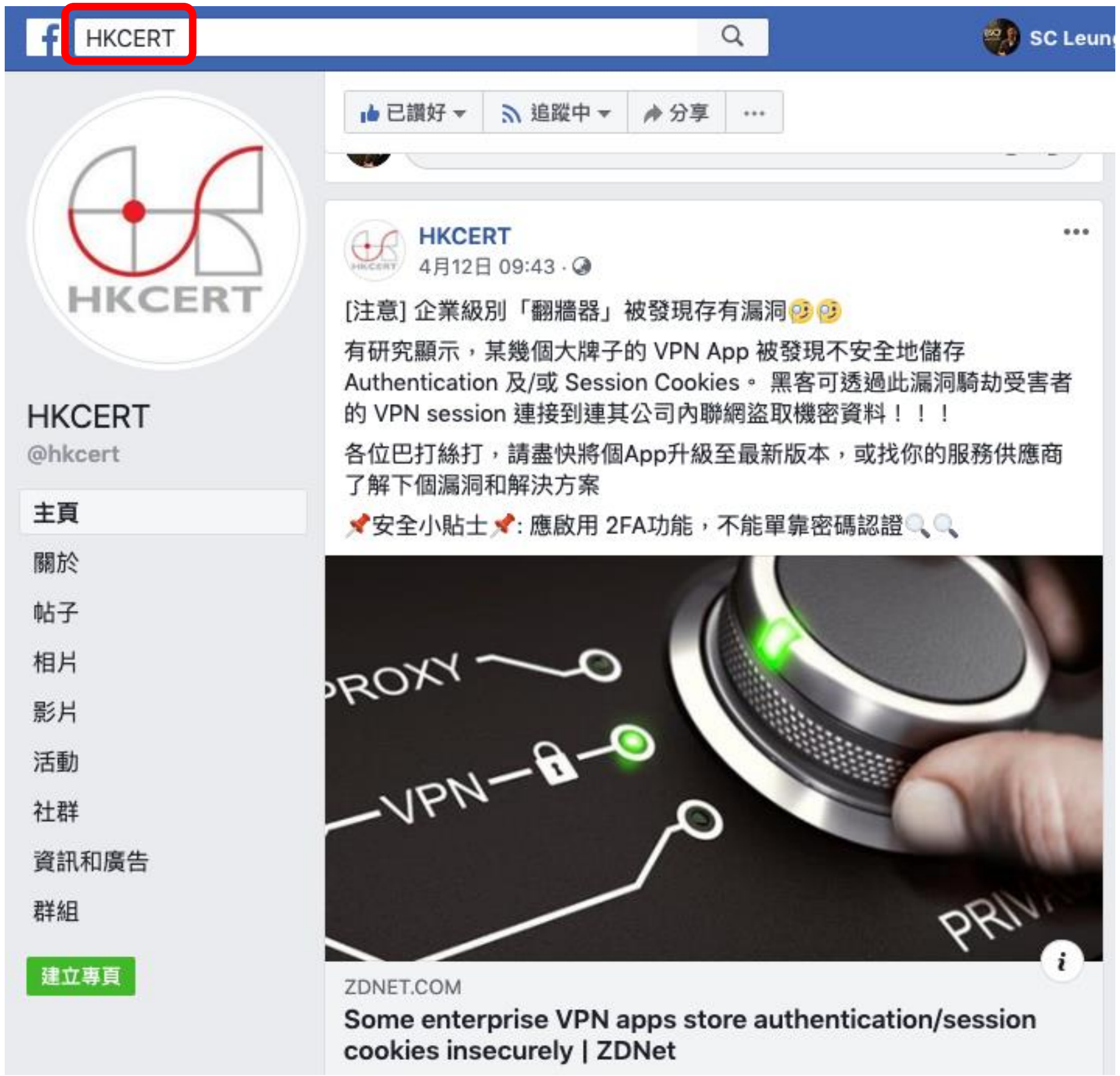
- 92,000 computers found to have installed infected games

HKCERT: Understanding and Tackling Supply Chain Attack
https://www.hkcert.org/my_url/en/guideline/18041201

Infestation New Z

HKCERT Facebook page

https://www.facebook.com/hkcert



HKCERT

SC Leun

已讚好 ▾ 追蹤中 ▾ 分享 ···

HKCERT

@hkcert

主頁

關於

帖子

相片

影片

活動

社群

資訊和廣告

群組

建立專頁

HKCERT

4月12日 09:43 ·

[注意] 企業級別「翻牆器」被發現存有漏洞🤔🤔

有研究顯示，某幾個大牌子的 VPN App 被發現不安全地儲存 Authentication 及/或 Session Cookies。 黑客可透過此漏洞騎劫受害者的 VPN session 連接到連其公司內聯網盜取機密資料！！！

各位巴打絲打，請盡快將個App升級至最新版本，或找你的服務供應商了解下個漏洞和解決方案

📌安全小貼士📌: 應啟用 2FA功能，不能單靠密碼認證🔍🔍

ZDNET.COM

Some enterprise VPN apps store authentication/session cookies insecurely | ZDNet

Q & A