國家層級的資安威脅與應處

-政府資安防護與推動

howard@ey.gov.tw
行政院資通安全處
110年11月

智慧生活，創意無限

自由時報

即時 熱門 政治 社會 生活 健康 國際 地方 蒐奇 影音 財經 娛樂 汽車 時尚 體育 3C 評論 玩咖

路跑+GPS 日男用足跡寫下愛台灣

志水直樹在台北跑出日本愛台灣字樣（見圖），並到花蓮跑出花蓮加油字），為地震災民打氣。（記者鄭名翔翻攝）

志水直樹在台北跑出日本愛台灣字樣，並到花蓮跑出花蓮加油字樣（見圖），為地震災民打氣。（記者鄭名翔翻攝）

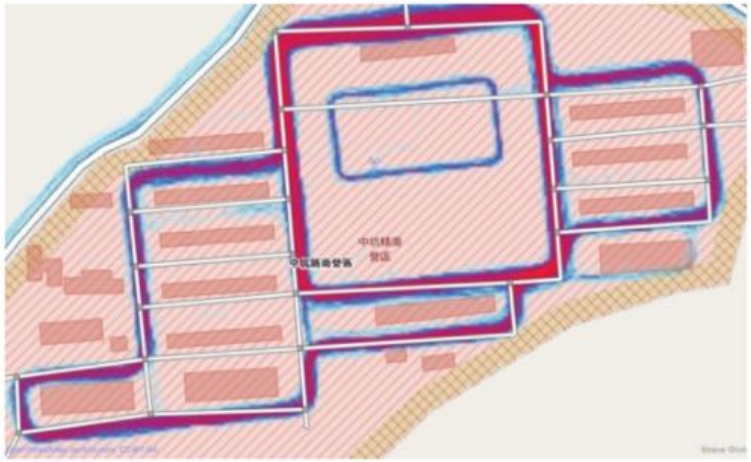
2018/05/07 06:00

感念台灣協助311日本大地震

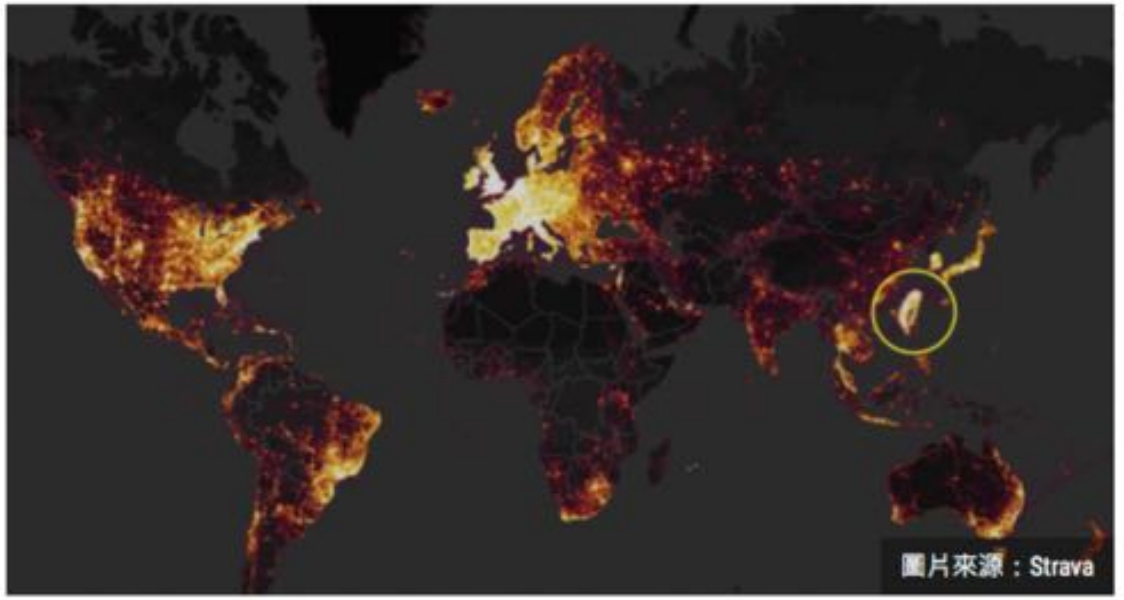
資料全都露

健身App「Strava」讓軍事機密大曝光，台灣營區和監獄也全都露

2018.01.31 by 科技新報 Technews



宜蘭監獄的固定巡邏路線，



> 健身追蹤應用程式 Strava可讓用戶記錄自己運動的路線，一般人記錄倒沒什麼關係，不過軍人的詳細紀錄卻讓世界各地軍事基地、哨點位置及人員配置等機密曝光。

資料全都露

健身APP洩密 美軍嚴格禁止戰區軍人私用GPS

23:45 2018/08/09 | 中時新聞網 | 盧伯華

69國軍情人員行蹤全都露 只因用了知名健身App

著名健身應用程式Strava公布其用戶的跑步熱點時，無意間洩漏了衝突地區美軍與軍事基地的位置與活動狀況，引發五角大廈對洩露軍事機密的擔憂。圖為GPS所繪出的用戶跑步路線圖。（圖／推特@Nathan Ruser）

2020 資安事件(1/2)

- 英國倫敦外匯交易公司Travelex遭勒索軟體Sodinokibi攻擊
- Magnallium駭客組織入侵美國電廠、煉油及天然氣公司網路

1月

- 以色列選舉系統因委外廠商設計疏失產生漏洞導致選民資料外洩
- 網路攻擊者以武漢肺炎名義散發電子郵件，企圖發動惡意攻擊

2月

- 歐洲電能組織辦公室IT系統遭惡意攻擊
- 捷克新冠肺炎篩檢中心遭勒索軟體攻擊

3月

- BGP劫持事件導致全球約200家CDN供應商流量導向俄羅斯
- 舊金山國際機場網站遭駭客掛碼竊取使用者帳密

4月

- 供應鏈攻擊鎖定GitHub開源軟體專案駭侵
- 泰國最大電信業者AIS數千萬用戶即時網路瀏覽資料外洩
- NAS廠商產品QNAP傳多項漏洞

5月

- 印度資安業者BellTroX涉非法監控數萬個電子郵件
- UPnP協定存在CallStranger漏洞
- 全美逾200所警局與情資整合中心之機敏資料外洩

6月

2020 資安事件(2/2)

- 駭客利用區塊鏈技術隱匿行蹤，鎖定Docker環境建置殭屍網路
- 推特大批名人帳號被駭，用來發送比特幣詐騙訊息

- 阿根廷移民署遭植入Netwalker勒索軟體
- 微軟Elasticsearch伺服器遭駭客攻擊刪除6.5TB用戶資料

- 西班牙網路軟體開發商Prestige Software雲端伺服器配置錯誤，造成至少10萬用戶機敏資料外洩
- 駭侵組織Cicada對日本組織發動大規模駭侵，掌握內網AD控制權

7月

8月

9月

10月

11月

12月

- 駭客透由Tor網路惡意節點，攔截置換傳輸資訊以竊取比特幣
- 紐西蘭證券交易所遭DDoS攻擊
- 逾20萬中國傳音所生產手機預載廣告詐騙程式

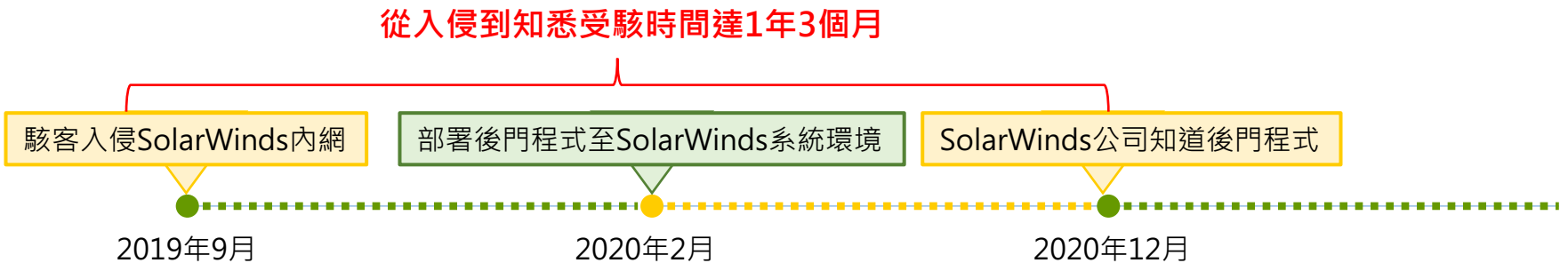
- 韓國多家銀行遭受UDP Flood DDoS分散式阻斷服務攻擊
- 網路券商Robinhood用戶帳號遭駭，部分用戶資產遭盜賣

- 駭侵組織利用Zerologon漏洞攻擊日本企業全球據點
- APT駭侵團體以最新macOS後門惡意軟體發動攻擊
- SolarWinds產品Orion遭駭，影響33000個公私營部門

2020年 SolarWinds供應鏈攻擊事件

零信任(Zero Trust)網路

- 從防火牆、路由器到伺服器，都可以在單一介面進行**統一管理與監控**的系統
- 攻擊手法—將**委外廠商**的平臺當成入侵目標對象的**跳板**
  - 駭客**入侵**SolarWinds Orion平臺，**植入惡意程式**，並打包**部署**到客戶環境中
  - **蒐集情資**，包括所在的伺服器、橫向的伺服器資訊、公司資訊等，且入侵軌跡皆會加密且自我刪除
- 影響—美國多個政府組織、資安業者、大型科技公司(包括Microsoft、VMware)等33,000個公私營部門都受影響，且相關電子郵件長期受到偷窺監視

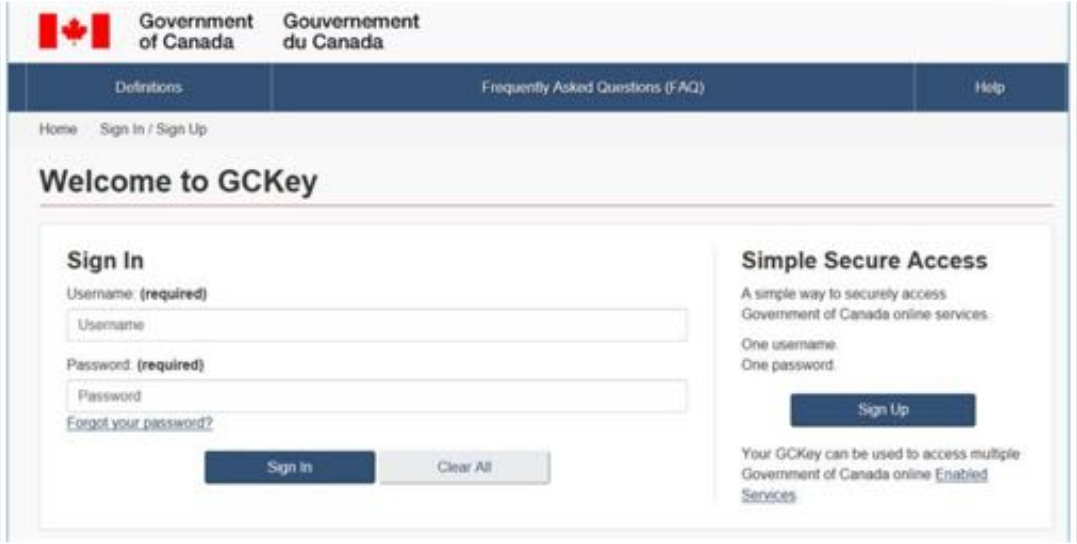


2020年中國APT駭客鎖定日本組織發動攻擊

- 攻擊手法
  - 利用名為Zerologon之**高風險資安漏洞**進行攻擊，掌握內網服務目錄網域(Active Directory, **AD**)之**控制權**
- 影響
  - 攻擊目標為日本汽車、製藥及機械製造業者，及其位於美、英、法、德、台、韓及新加坡等16國之分公司，**竊取**企業**機敏資訊**

2020年加拿大政府網站遭駭

- 攻擊手法
  - 駭客利用**已外洩**的**資料**，加上部分使用者會在多項服務使用**同樣密碼**的安全弱點，破解1萬多個加拿大政府以及當地國稅局線上服務的用戶憑證
- 影響
  - 上萬用戶憑證遭竊，駭客並鎖定身分驗證服務(GCKey)憑證與國稅局帳號發動攻擊，約有9千多筆憑證與5千多筆帳號遭破解
    - ◆一組GCKey可用以存取30種政府服務 (在3,800萬的加拿大人口中，已有1,200萬擁有GCKey憑證)



2021年美國佛州淨水處理廠遭駭事件

- 攻擊手法
  - 駭客日常作業所使用的TeamViewer(**遠端**控制**軟體**)**漏洞**來存取工廠的控制系統，更改淨水廠控制系統氫氧化鈉濃度至超標數值(100 ppm→11,100 ppm)
- 損害
  - 幸由工作人員及時發現異常並手動進行修正，因而未危及上千萬居民的飲用水安全

照片來源：cybernews

iThome

新聞

https://www.ithome.com.tw/news/142729

Windows 7、TeamViewer、共用密碼、沒防火牆四大安全缺陷，造成美國淨水廠遭駭

FBI也警告使用微軟已不支援的Windows 7、弱密碼及TeamViewer等桌面共享軟體有高風險，各界應以淨水廠遭駭事件為戒，檢查內部網路和存取政策

讚 6.4 萬 按讚加入iThome粉絲團 讚 697 分享

文/ 林妍溱 | 2021-02-12 發表

FBI本周發出的民間產業通知（Private Industry Notice，PIN），警告使用微軟已不支援的Windows 7、弱密碼及TeamViewer等桌面共享軟體有高風險，呼籲民間和聯邦政府機關檢查內部網路和存取政策。（圖片來源 / https://us-cert.cisa.gov/ncas/alerts/aa21-042a）

2021年美國油管公司遭勒索軟體攻擊事件

- 攻擊手法
  - 透過**未修補**的**漏洞**進入受害電腦或是寄送夾帶病毒的**釣魚郵件**，誘騙內部人員下載並安裝病毒程式
- 損害
  - 駭客聲稱**取走**100GB的資料，並**加密**油管公司的**資料**
  - 為避免系統失能並阻止病毒對內部系統進一步破壞，預防性**中斷油管6天**進行搶修，造成部分地區原油價格上漲
  - 支付 75 個比特幣，總計**約 440 萬美元**(約台幣 1.23 億元)
    (後追回230萬美元，約台幣6,370萬元)
  - 面臨業者訴訟求償

魚叉式網路釣魚郵件範例

圖片來源：udn

2021年監控公司Verkada遭駭

- 攻擊手法
  - 在網路上公開資訊中找到「**超級管理員(Administrator)**」帳密，進而輕鬆進入公司系統
- 影響
  - 15萬臺監視器(警察局、醫院、監獄、學校及Tesla等)即時監控畫面外流，甚至能利用臉部辨識技術監看人員

圖片來源：Verkada 情境示意圖

威脅潛伏

世界經濟論壇2021全球風險調查報告

高 風險發生影響性

風險發生可能性 高

10大影響風險

1. 傳染病
2. 緩解氣侯變化行動失敗
3. 大規模殺傷性武器
4. 生物多樣式喪失
5. 自然資源危機
6. 人為環境災害
7. 民生危機
8. 極端氣侯
9. 債務危機
10. 資訊基礎建設破壞(2020年排名第6)

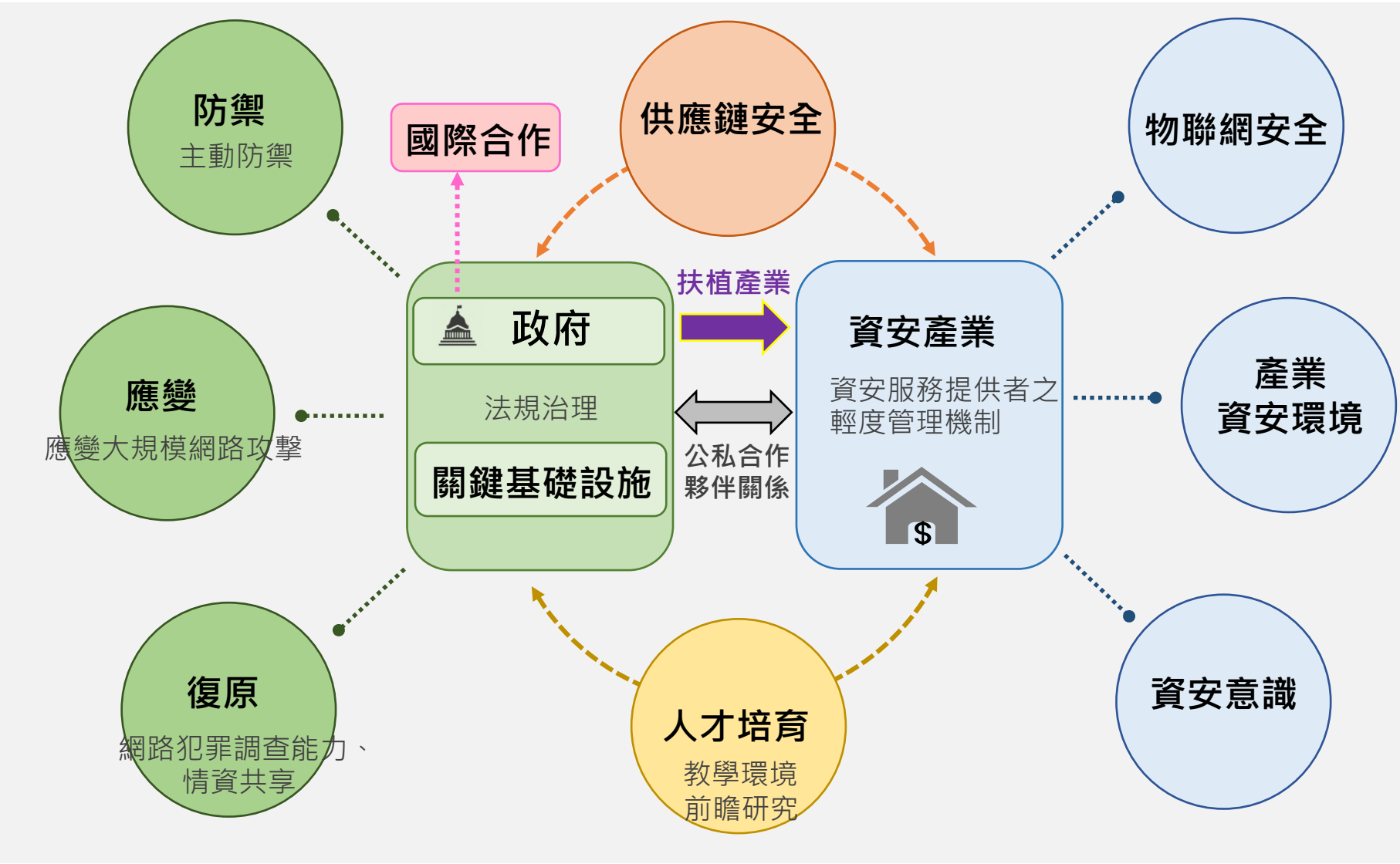
10大可能長期風險

1. 極端氣侯
2. 緩解氣侯變化行動失敗
3. 人為導致的環境災害
4. 傳染病
5. 生物多樣式喪失
6. 集權控制數位資源
7. 數位落差
8. 國際關係裂痕
9. 資安防護失敗
10. 民生危機

紅色：科技因素
藍色：2021年新增因子

資料來源：The Global Risks Report 2021 16th Edition, World Economic Forum

國際資安戰略發展分析


防禦
主動防禦
國際合作
供應鏈安全
物聯網安全
扶植產業
政府
法規治理
關鍵基礎設施
資安產業
資安服務提供者之
輕度管理機制
公私合作
夥伴關係
應變
應變大規模網路攻擊
產業
資安環境
復原
網路犯罪調查能力、
情資共享
人才培育
教學環境
前瞻研究
資安意識

凡事皆有價

SEPTEMBER 2019

THE ARMOR 2019 BLACK MARKET REPORT

A LOOK INSIDE THE DARK WEB

Extracts from one hacker's price list:

Black Market Service and Goods	Cost
U.S. Visa/Mastercard data (U.S. prices)	$15-$20 dollars (rising to $25-$30 for BIN number and DOB)
US Fullz data (Full ID package)	$30-$40
Generic Ransomware	$225 – $660
Ranion (Ransomware-as-a-service)	$120 per month
MegaCortex	$1000 or 1000 Euros and 10% of ransom
Unhacked Remote Desk Protocol Servers in multiple countries	$20 per RDP server
Amazon gift card with $1000 balance	$100
ATM skimmers	£500 to $1500
DDoS attack	$60 per hour
Money Transfer Services (PayPal, Bank Transfer, Western Union and Skrill)	Average of $800 for a balance of $10,000
Changes to credit history	From $130

我們有不同嗎？

個資外洩

小白機洩1億筆個資！千名房仲遭查　創始人被抓警逮64人

2021/08/18 10:20:00

追蹤三立：

記者陳啓明／台北報導

房仲神器（俗稱小白機）號稱擁有全國人民個資，今年3月就有地政士爆料有不肖人士在市場兜售，新北地檢署立案調查後，陸續約談超過千名房仲，經長時間蒐證，發現當過房仲的溫、林男涉案，2人設計個資查詢程式，俗稱小白機，蒐集屋主個資，把程式以8千到5萬的價格賣給各品牌房仲，洩漏1億多筆屋主個資，檢警日前收網，共計逮捕64名嫌犯，全案訊後依違反個資法移送法辦。

勒索軟體

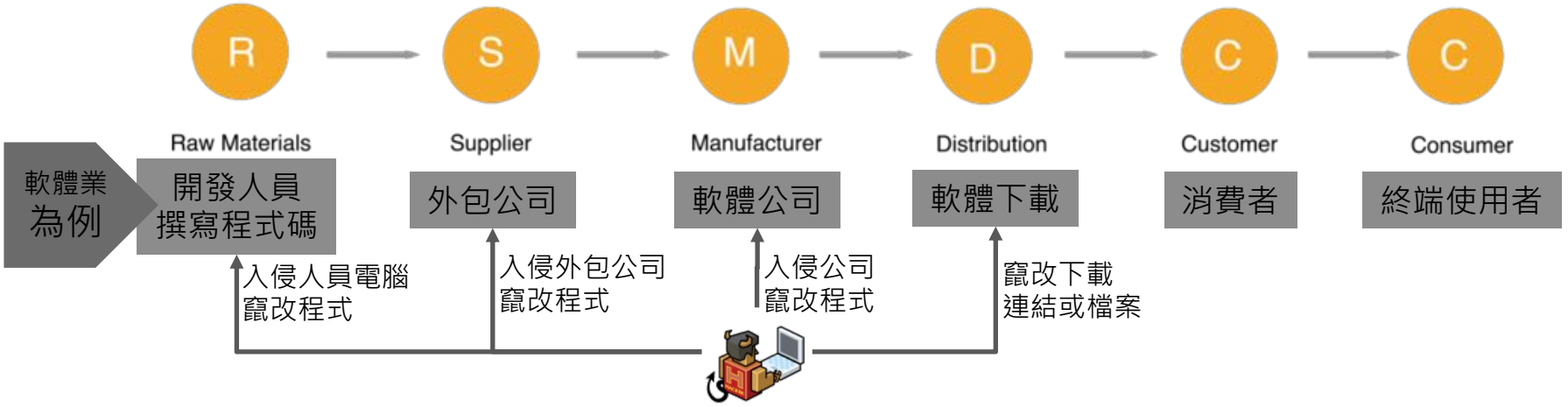
WannaCry進化為蠕蟲，勒索軟體殺傷力大增

加密型勒索軟體在近年成為常見的資安威脅，然而，卻未曾有過一個勒索軟體能像發生於5月12日的WannaCry一樣，在短短的一個周末就讓全球超過150個國家、數十萬臺電腦被攻擊

文/ iThome | 2017-05-22 發表

供應鏈攻擊持續發生

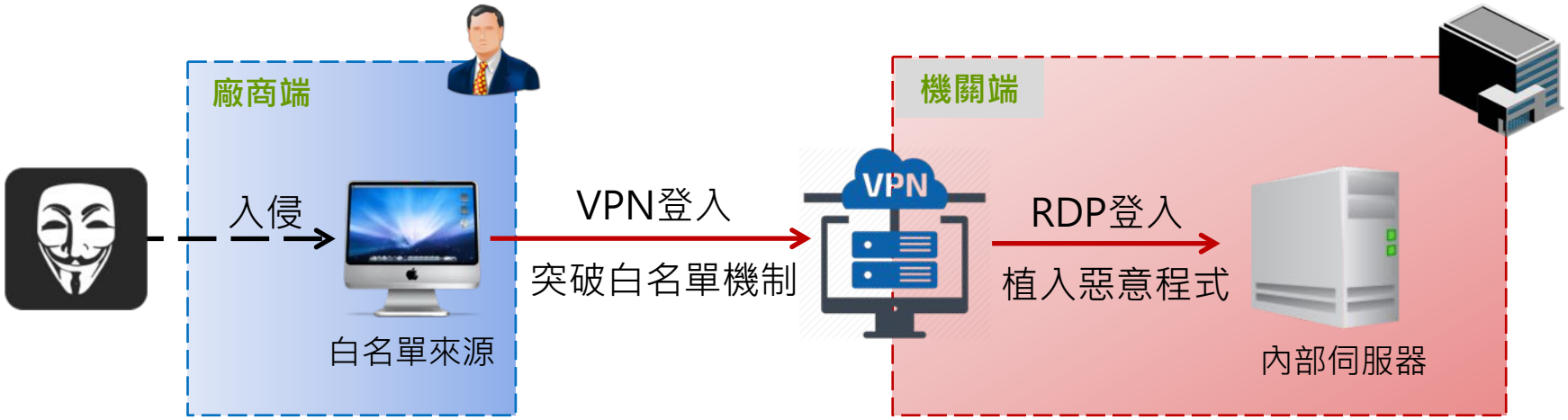
- 供應鏈泛指組織企業將產品或服務，提供給終端使用者的過程與活動，駭客通常鎖定供應鏈中安全防護較弱的環節進行攻擊
  - 駭客藉由入侵特定軟/韌體開發公司或人員電腦，進行竄改程式或下載連結等行為，造成大範圍的感染與擴散
  - 最大特色是利用**受信任的管道**進行散播
  - 入侵軟體開發廠商後，可以其做為跳板，滲透客戶組織



資料來源：https://www.wikiwand.com/en/Supply_chain_attack#/citenote30

供應鏈攻擊案例

- 發布中繼站連線警訊通知機關應處，經日誌分析比對主機鑑識結果後發現，攻擊來源為機關維護廠商
  - 駭客透過白名單VPN機制，以遠端桌面方式登入機關主機植入惡意程式



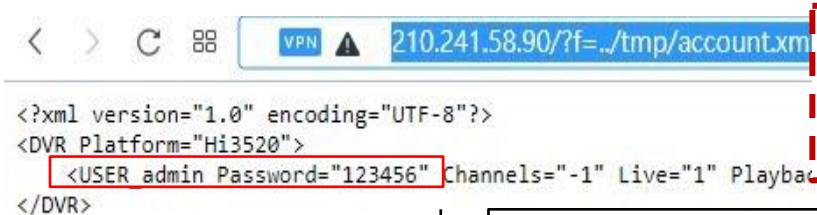
DVR入侵案例分析

- 近期發現大量機關有異常下載行為，經分析為視訊監控錄影主機(DVR)被駭，因而下載ZBOT或Mirai Bot惡意檔案
  - Icatch (可取國際)、HME(環名)及Fine (上敦企業)DVR被揭露，存有預設帳密、命令注入漏洞及任意檔案讀取漏洞可利用

- 韌體帳密
  root/icatch99
  report/8JgoSR8K50
- 預設帳密
  admin/123456

1.韌體內建帳密，可登入

2.登入後 ，執行命令



受害主機集中於兩網段
- 117.56.0.0
- 61.60.0.0

3.執行帳密傾印的結果

我們的現況是怎麼樣？

機關資安責任等級核定情形

- 資通安全管理法自108年1月1日開始實施
- 核定之納管對象：**7,706個**(110年2月17日止)

公務機關

- 中央與地方機關(構)
- 公法人

(不包括軍事機關及情報機關)

特定非公務機關

- 關鍵基礎設施提供者
- 公營事業
- 政府捐助之財團法人

機關類型	A級	B級	C級	D級	E級	總數
中央機關	44	144	365	315	113	981
地方政府	0	106	532	4,981	679	6,298
特定非公務機關	46	122	155	84	20	427
全部類型	**90**	**372**	**1,052**	**5,380**	**812**	**7,706**

政府機關資安事件統計

	一級	二級	三級	四級	總計
108年	254	45	11	0	310
109年	451	65	9	0	525
110年*	427	35	11	0	473

*110年統計至8月31日

109年政府機關重大資安事件通報

項次	通報時間	通報機關	事件說明	事件根因
1	109/2/19	教育體系	網站**設計漏洞**遭外部使用者不當方式存取，下載約7萬筆個人資料。	人為疏失
2	109/5/13	地方政府	表單試算表**權限設定錯誤**，導致可公開檢索編輯所蒐集之民眾個人資料。	人為疏失
3	109/7/17	中央機關	資料中心網路服務異常，影響雲端中心主機對外服務。	設備問題
4	109/8/8	地方政府	機關使用Google表單供民眾登記，惟表單**權限設定錯誤**，導致可公開瀏覽民眾個人資料。	人為疏失
5	109/9/2	中央機關	機關網站存在**設計漏洞**，接獲外部情資，表示可繞過網站身分驗證機制，下載個人資料。	人為疏失
6	109/9/3	醫療體系	機關主機遭植入勒索病毒，影響核心系統運作。	駭客入侵
7	109/9/10	中央機關	機關涉及CI業務系統運作異常，影響全台對民眾服務。	駭客入侵
8	109/10/14	教育體系	因人員**操作不慎**，誤將民眾個人資料夾帶於電子郵件寄出。	人為疏失
9	109/11/1	中央機關	系統**不當變更**，致包含民眾個資之敏感資料外洩，估計約有51筆資料遭異常存取。	人為疏失

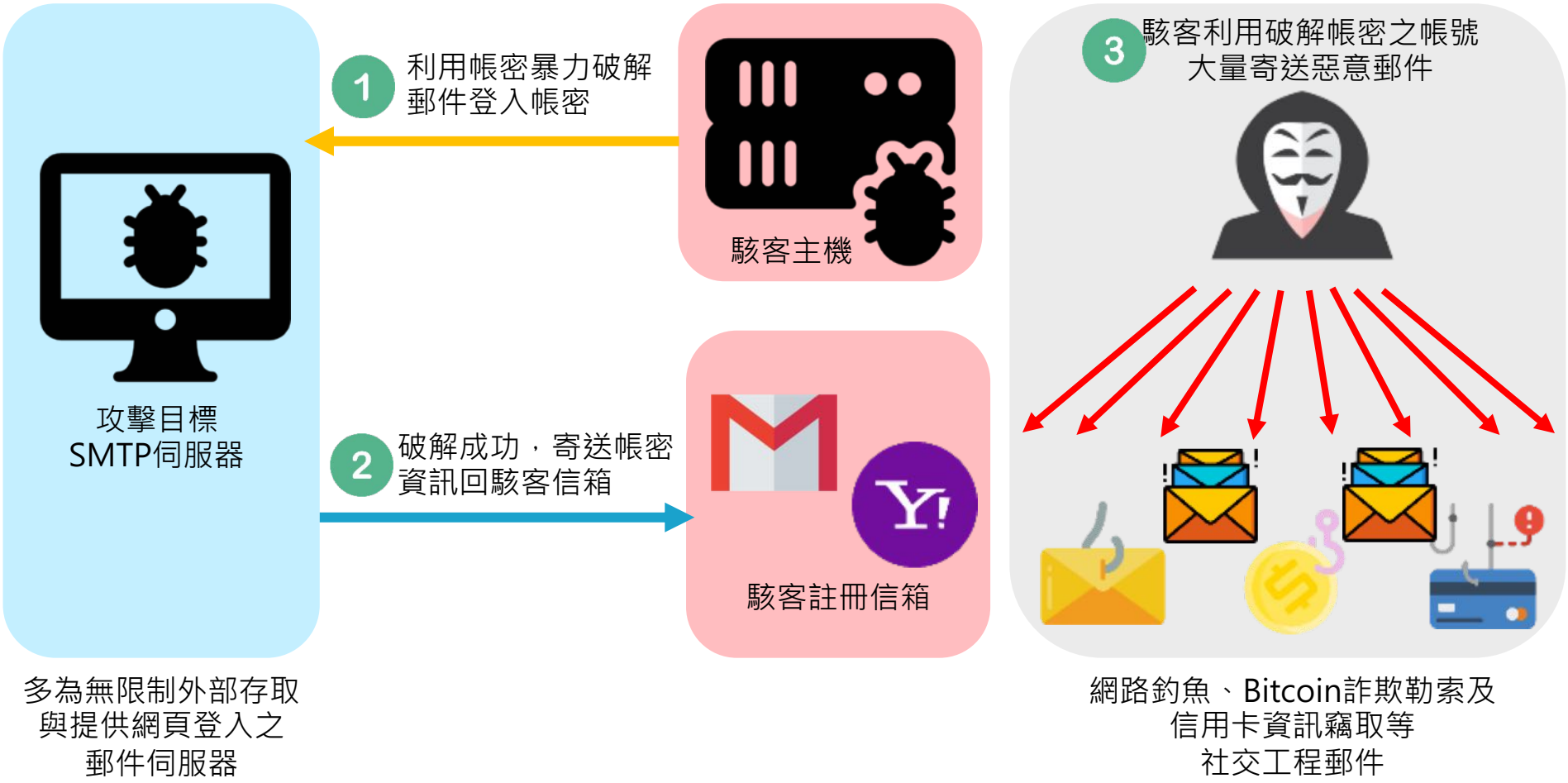
- 調整資訊服務採購契約範本，讓機關據以要求廠商負起資安責任
- 要求機關原則禁止遠端存取，並應在網站建置時就導入資安概念

110年政府機關重大資安事件通報

項次	通報時間	通報機關	事件說明	事件根因
1	110/1/25	教育體系	網站遭外部使用者不當存取方式，下載約1.3萬筆個人資料。	人為疏失
2	110/2/3	地方政府	廠商於活動網站發布抽獎資訊時，**誤放連結**使民眾資料外洩。	人為疏失
3	110/2/24	司法體系	資料庫服務中斷，超過可容忍中斷時間。	設備問題
4	110/3/26	教育體系	承辦人**未將敏感資料進行遮罩**即將包含個資資料上傳至網站。	人為疏失
5	110/3/26	教育體系	承辦人**未將敏感資料進行遮罩**即將包含個資資料上傳至網站。	人為疏失
6	110/4/16	教育體系	網站**存在程式漏洞**遭外部使用者不當利用，下載約650筆個人資料。	人為疏失
7	110/4/22	教育體系	來自國外異常連線以AP管理者帳號登入網頁，惟該職員休假中，疑似因**弱密碼**導致入侵。	人為疏失
8	110/5/10	中央機關	涉及CI維運系統服務中斷。	設備問題
9	110/6/4	教育體系	因線上報名**程式漏洞**導致部份個資外洩。	人為疏失
10	110/8/25	教育體系	線上表單權限**設定不當**導致學生填報資料外洩。	人為疏失
11	110/9/6	教育體系	線上表單權限**設定不當**導致填報資料外洩。	人為疏失

今年至今尚無入侵事件，多為人為疏失造成個資外洩，已要求加強人員對資料的保護

郵件帳密爆破攻擊示意



多為無限制外部存取
與提供網頁登入之
郵件伺服器

網路釣魚、Bitcoin詐欺勒索及
信用卡資訊竊取等
社交工程郵件

受駭郵件帳密列表

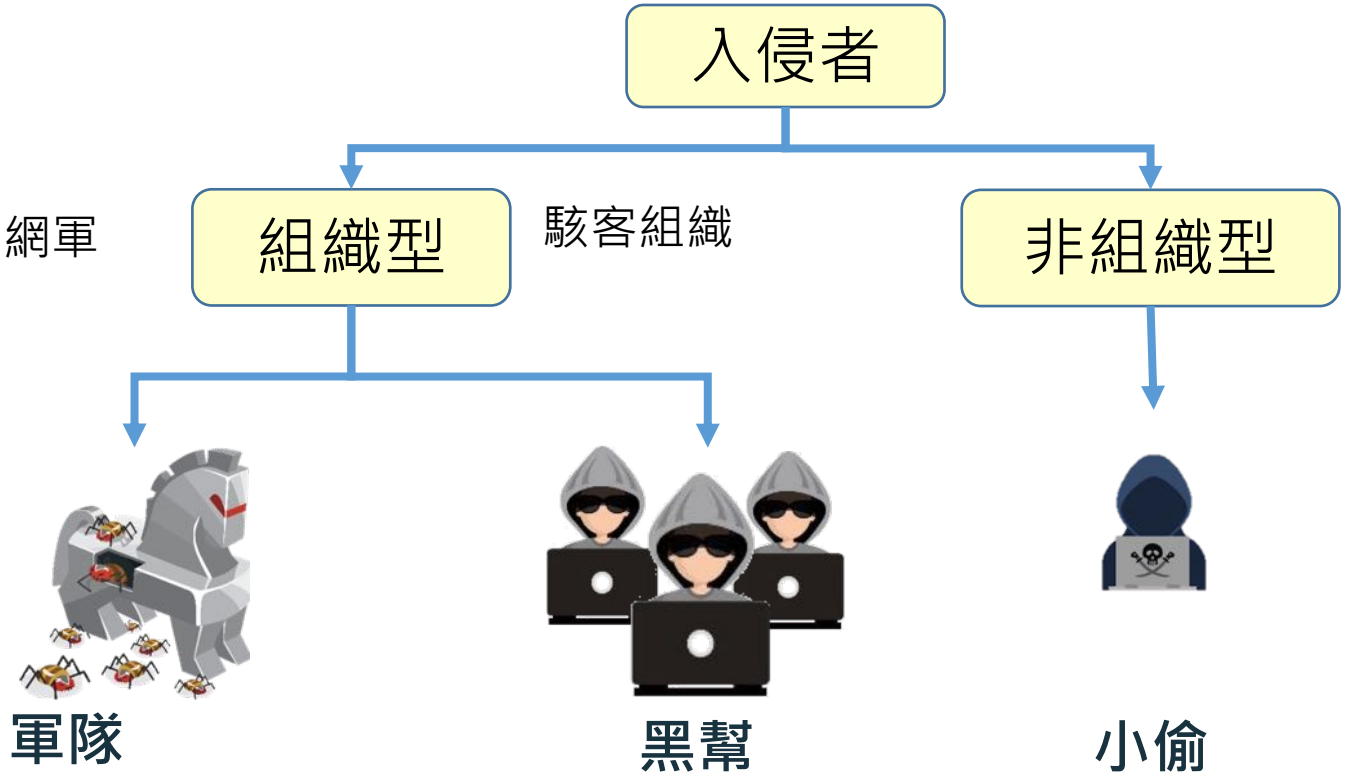
- 目前發現34個機關共190組郵件帳密可能已遭竊取，其中28個機關共143組帳密皆透過主旨回傳至攻擊者，前十大已洩露密碼統計如下

10大遭竊密碼		
No.	密碼	數量
1	密碼同帳號	33
2	123	24
3	123456	14
4	Aa123456	3
5	0000	2
6	03031229	1
7	1qaz@WSX	1
8	asdf1234	1
9	P@ssw0rd	1
10	123456789	1

註：A級機關： 1
B級機關： 6
C級機關：16
D級機關： 5

我們面對什麼？

資安攻擊的來源及動機



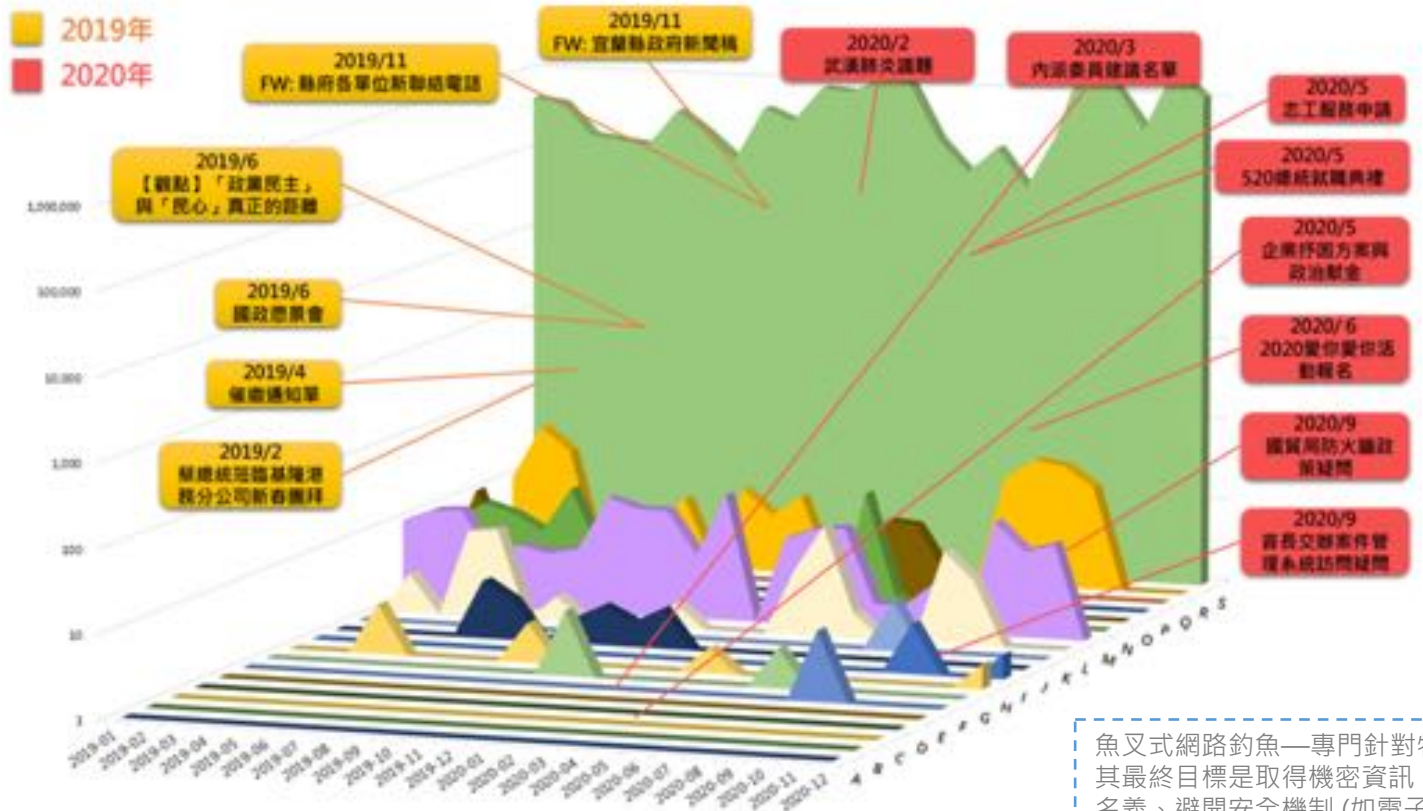
動機：

政治目的、經濟利益、個人名聲

政府領域APT攻擊趨勢

➢109年政府領域APT攻擊趨勢可歸納為三波攻擊行動

- 年初利用COVID-19議題與政府機關採購主旨進行魚叉式釣魚郵件攻擊
- 年中利用520總統就職典禮，針對不同機關與重要人士寄送惡意電子郵件
- 雙十國慶期間，利用系統相關問題主旨對政府機關業務負責人員發動攻擊



魚叉式網路釣魚—專門針對特定對象的網路釣魚，其最終目標是取得機密資訊，技巧包括：假冒他人名義、避開安全機制 (如電子郵件過濾及防毒) 等

109年中油案攻擊時間序

2018年7月6日

中油全球資訊網子網站有惡意程式出現，駭客長期潛伏

2020年3月19日

中油全球資訊網站向內部電腦發起異常連線

2020年3月22日

駭客成功入侵網域工作站，對內產生大量異常連線並觸發警訊通報

2020年3月23日

兩臺電腦被植入後門程式Cobalt Strike，作為入侵跳板

2020年5月4日

駭客竊取管理者帳密登入AD伺服器群，建立排程並透過GPO派送病毒至受管理電腦；凌晨12:10啟動勒索軟體，資料均遭加密

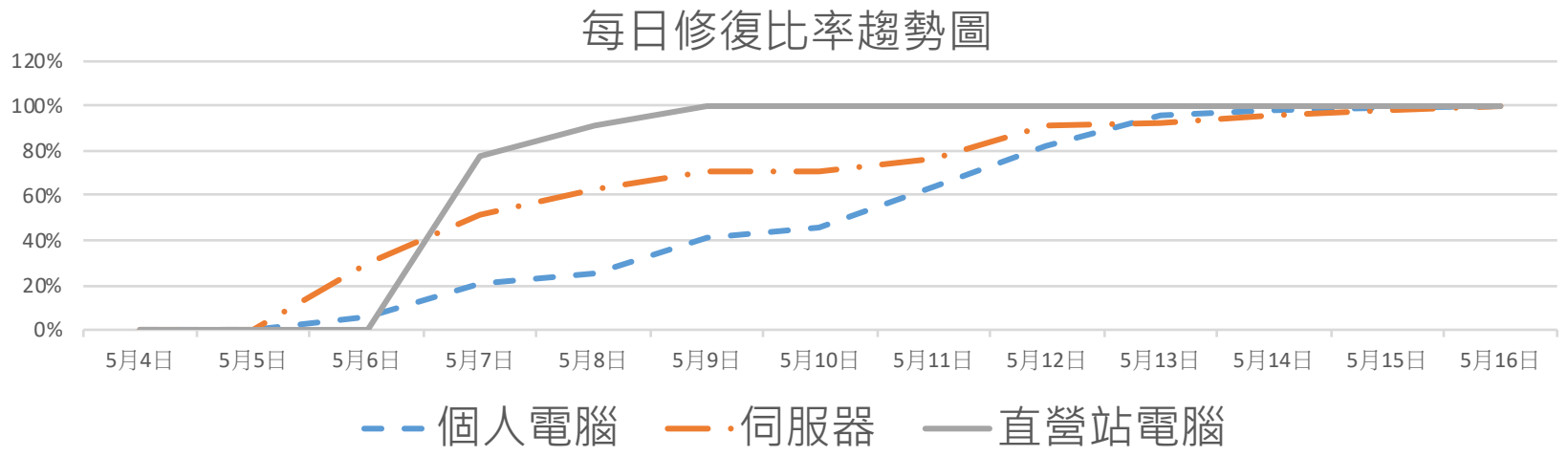
109年中油案影響範圍

➢營運面

- 加油站服務改為離線作業，不影響供油
- 車隊卡、捷利卡、會員卡系統服務中斷，於5/4修復
- 中油pay服務中斷，於5/5修復
- 郵件系統及公文系統等內部系統服務中斷

➢生產面

- 關鍵基礎設施工控系統未受影響。

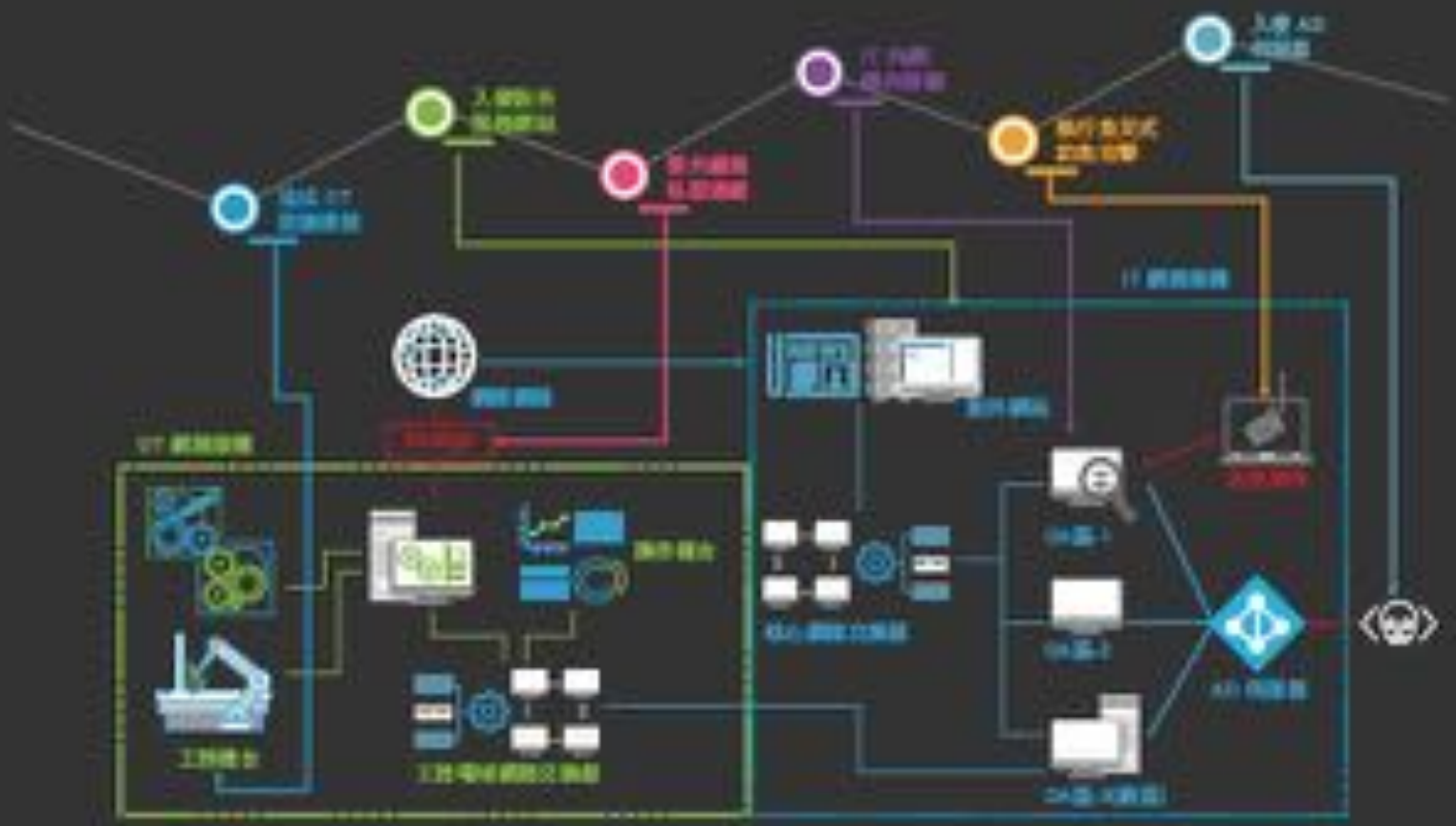


問題的根因是什麼？

關鍵基礎設施受駭可能危害

CODE 2021

關鍵基礎設施可能入侵管道

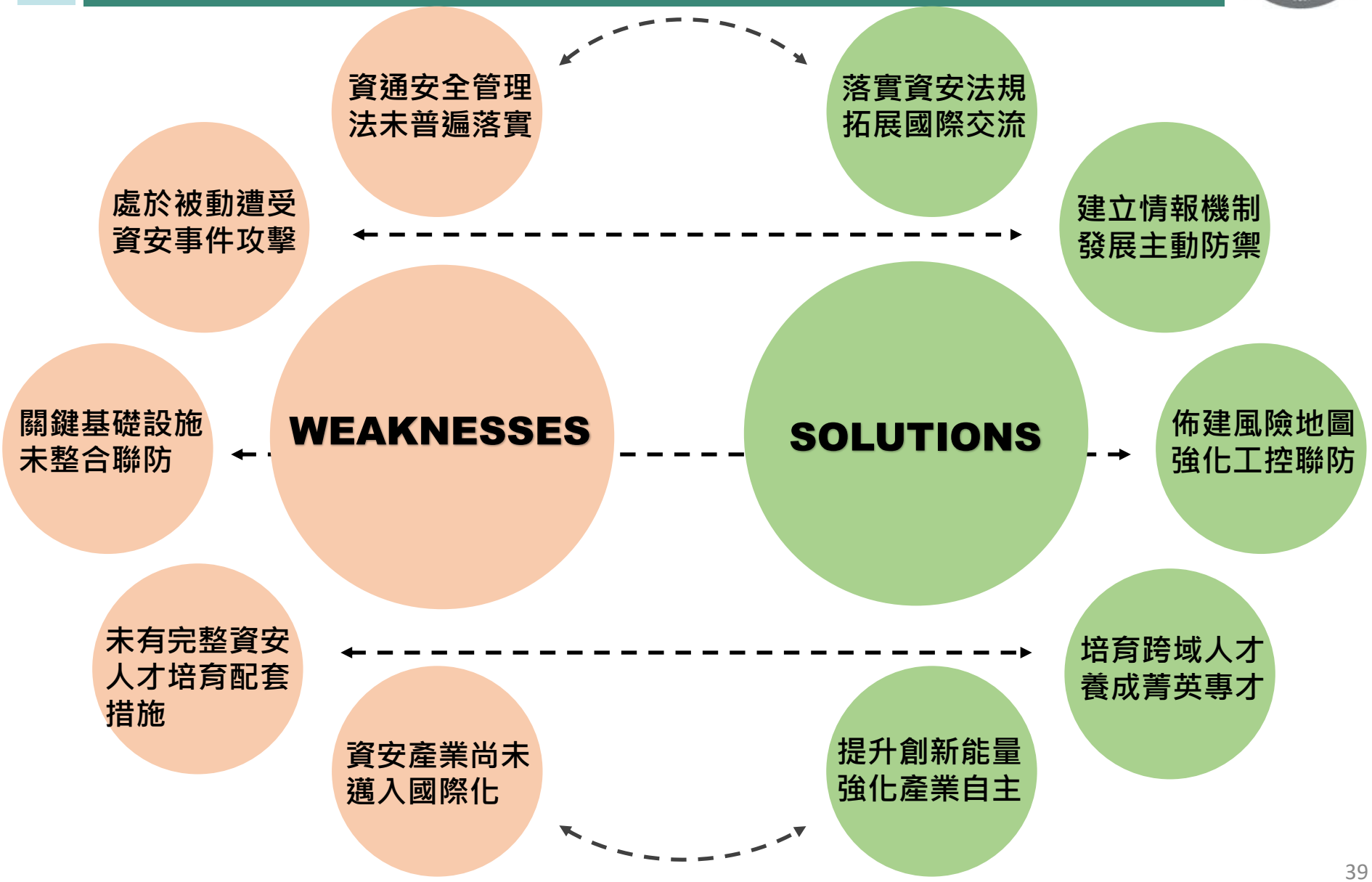


CODE 2021

政府機關威脅情勢綜合評估

- APT惡意電郵為組織型駭客主要攻擊手法，各機關須持續加強人員資安意識，防範社交工程電子郵件攻擊
- 行動裝置或物聯網設備遭利用擴散惡意程式或殭屍網路，建議使用行動裝置應遵守相關資安規範，同時妥善管理物聯網設備
- 重大資安事件仍以個資外洩造成之衝擊為主，多肇因於網站或權限設計不當，建議機敏資料非必要不得置於公開網站
- 部分資安事件起因「廠商維護環境或管理疏失」，顯示委外廠商資安管理之重要性，應落實委外管理機制
- 資安事件缺乏相關紀錄，以致無法有效針對根因進行改善，顯示對於日誌紀錄保存仍有改善空間

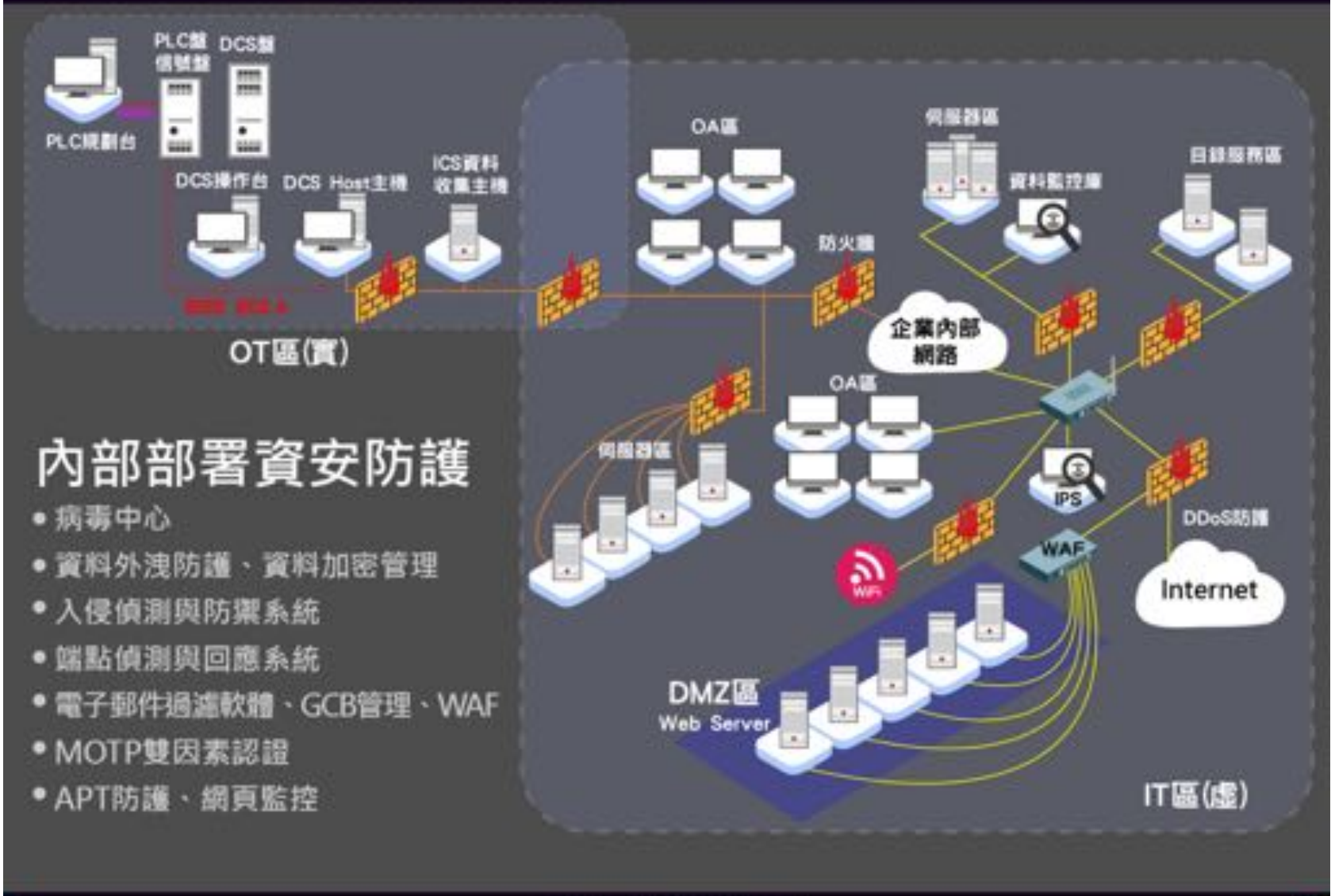
問題與對策


資通安全管理
法未普遍落實
落實資安法規
拓展國際交流
處於被動遭受
資安事件攻擊
建立情報機制
發展主動防禦
關鍵基礎設施
未整合聯防
WEAKNESSES
SOLUTIONS
佈建風險地圖
強化工控聯防
未有完整資安
人才培育配套
措施
培育跨域人才
養成菁英專才
資安產業尚未
邁入國際化
提升創新能量
強化產業自主

CII資安防護建議

CODE 2021

資安防禦縱深示意圖



內部部署資安防護

- 病毒中心
- 資料外洩防護、資料加密管理
- 入侵偵測與防禦系統
- 端點偵測與回應系統
- 電子郵件過濾軟體、GCB管理、WAF
- MOTP雙因素認證
- APT防護、網頁監控

可以怎麼做？

基本問題

01 資安規範難以落實

① 加強同仁資安意識
② 督導各機關落實

02 CI防護待加強

① 尋求OT專才
② 強化CI防護

03 防護架構缺乏整體性

① 建立整體防護網
② 建立整體防護策略

04 機關架構紊亂

① 向上集中到部會
② 建立一致性/集中化管理

加強資安整備(1/2)

- 強化漏洞修補
  - 隨時注意重大漏洞訊息，即時修補防護
  - 導入VANS系統，掌握即時訊息
  - 執行滲透測試與紅隊演練，主動發掘資安防護漏洞
- 完善備援機制
  - 做好系統備援，確保服務不中斷
  - 除熱備援與異地備援，宜同時考量資料離線備份，以防勒索軟體攻擊

- 落實系統紀錄保存
  - 妥善規劃保存系統紀錄，以利資安事件鑑識分析
  - 系統紀錄應包含應用程式與資料庫等紀錄訊息，以利分析事件根因，改善資安管理

加強資安整備(2/2)

機敏資料採取加密、遮罩、混淆等保護機制

使用高安全性之加密簽章憑證
使用加密傳輸協定傳遞資料，採行更安全加密演算法

定期分析資料庫稽核紀錄，發現潛在異常行為

啟用帳號與密碼原則設定，強化帳號密碼安全性

精進縱深防禦(1/2)

- 落實黑名單部署
  - 於防火牆等資安防護設備定期更新黑名單，以技服中心提供黑名單為基礎，增列機關自有防護規則，確保資安防護即時有效
- 精進資安監控防護
  - 妥善規劃資安監控範圍，監控內外異常活動，即時告警
  - 加強關聯分析能量，提升資安監控防護有效性
- 落實權限控管
  - 人員帳號密碼採用最小權限原則，同時配合異常紀錄檢視，監控可疑活動
  - 資通系統權限設定，應納入上線前之檢驗項目
  - 加強供應商管理與來源管制，遠端連線原則禁止例外開放

精進縱深防禦(2/2)

- 針對供應商連線至機關內部環境應加強來源管制，遠端連線原則禁止例外開放

※雲端服務之使用不在此禁止範圍

行政院資安處110年3月2日院臺護字第1100165761號函

及時應變處理

- **阻斷APT竊密**
  - ●公務人員使用公開之雲端服務，應遵循機關之管理規範，並隨時通報異常事件，以利分析防護資安事件
  - ●機關之資安防護設備如 IPS/IDS 等，可部署APT攻擊偵測規則，及時阻斷駭客攻擊
- **完善系統紀錄收集保存**
  - ●妥善規劃保存系統紀錄，以利資安事件鑑識分析
  - ●系統紀錄應涵括應用程式與資料庫等紀錄訊息，以利分析事件根因，改善資安管理

公務機關資通訊產品使用原則

- 109年12月18日院臺護長字第1090201804A號行政院秘書長函諒達
- 公務用之資通訊產品**不得使用大陸廠牌**，且**不得安裝非公務用軟體**
- 個人資通訊設備不得處理公務事務，亦不得與公務環境介接
- 各機關應就已使用或採購之大陸廠牌資通訊產品**列冊管理**，且**不得與公務環境介接**，並儘速汰換
  - 大陸廠牌認定方式由機關「**從嚴認定**」

遠端存取控制機制

- 110年3月2日院臺護字第1100165761號行政院資通安全處函諒達
- 採「**原則禁止、例外允許**」方式辦理
  - 例外原則：地理限制、處理時效及專案特性等因素
    - 依資安法附表10落實遠端存取相關規定
    - 開放原則**以短天期為限**，並建立**異常行為管理**機制
    - 結束後，應**確實關閉**網路連線，並**更換**遠端存取通道(如 VPN)登入**密碼**

勿使用身分證字號作為使用者帳號密碼

- 105年11月30日院臺護字第1050185463號行政院資通安全處函諒達
- 身分證字號屬個資法規定之個人資料，各政府機關資訊系統**不應使用身分證字號做為帳號名稱**，亦**不可使用弱密碼做為使用者預設密碼**

落實資通訊產品資安驗證與管理措施

- 建議於**採購契約**文件中明訂安全性規範
  - ✓欲採購之資通訊產品(含硬體、軟體及服務)如已有相關資安檢測技術規範，應明訂需通過**資安驗證**
  - ✓產品**安全漏洞(CVE)**公布後，應**即時修補**或完成相關安全**配套**
    - ◘例如：乙方提供之無線路由器應取得物聯網資安標章證明
    - ◘例如：乙方提供之資通訊產品倘有公布CVE漏洞，應於甲方規定期限內完成修補或相關安全配套措施

- 國家通訊傳播委員會業透過「關鍵電信基礎設施資通設備資通安全檢測技術規範」建立具乙太網路介面之防火牆、交換器、路由器等資通設備之安全檢測規範

CVSS評分	完成CVE修補並出具檢測機構報告之時限
7.0以上	CVE披露日起14日內
4.0-6.9分(含)	CVE披露日起45日內
0.1-3.9分(含)	CVE披露日起6個月內

公務機關之資通安全管理

✓ 應訂定、修正及實施資通安全維護計畫§10
✓ 應訂定通報及應變機制§14 I

行政院

- 擘劃並推動國家資通安全政策
- 資通安全科技發展
- 國際交流合作及資通安全整體防護
- 定期公布國家資安情勢報告及資通安全發展方案

訂定

- 應提出年度資通安全維護計畫之實施情形§12
- 應提出改善報告§13 II
- 應通報資通安全事件§14 II
- 應提出資通安全事件之調查、處理及改善報告§14 III

上級或監督機關 ⇄ 下級或受監督機關

- 應稽核資通安全維護計畫實施情形§13 I

總統府、立法院、司法院、考試院、監察院、直轄市政府、直轄市議會、縣（市）政府及縣（市）議會

設置資通安全長§11

- ✓資安管理法施行細則§22
- ✓資安責任等級分級辦法§7
- ✓資安事件通報及應變辦法§ 14、18
- ✓維護計畫實施情形稽核辦法§ 7、13
- ✓資安情資分享辦法§8
- ✓公務人員獎懲標準§15、 §19

特定非公務機關之資通安全管理

	關鍵基礎設施提供者	公營事業、政府捐助之財團法人
資通安全維護計畫	①應訂定、修正及實施資通安全維護計畫§16 ②應提出資通安全維護計畫之實施情形§16 ③應提出資通安全維護計畫之改善報告§16	①應訂定、修正及實施資通安全維護計畫§17 ②得提出資通安全維護計畫之實施情形§17 ③應提出資通安全維護計畫之改善報告§17
通報應變	④應訂定通報及應變機制§18 ⑤應通報資安事件，並提出調查、處理及改善報告§18	

罰則 §20~§21

關鍵基礎設施(CI)提供者

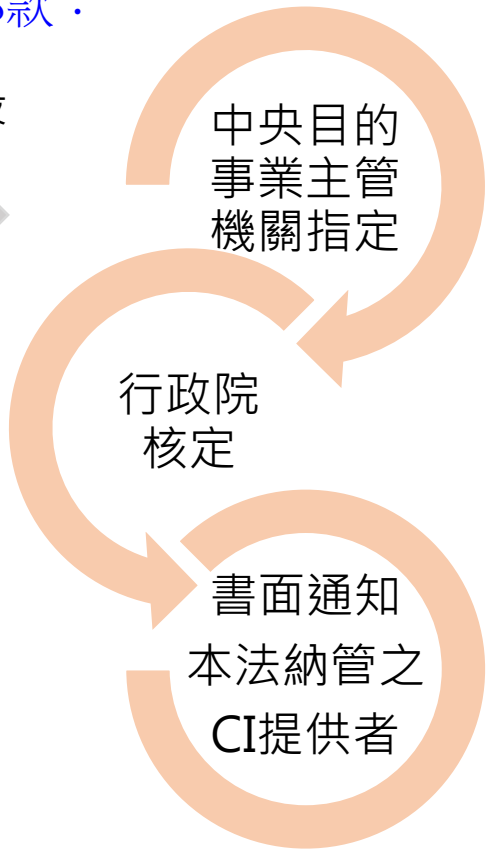
資通安全管理法第3條第7款：
關鍵基礎設施(CI)

定期檢視並
公告領域

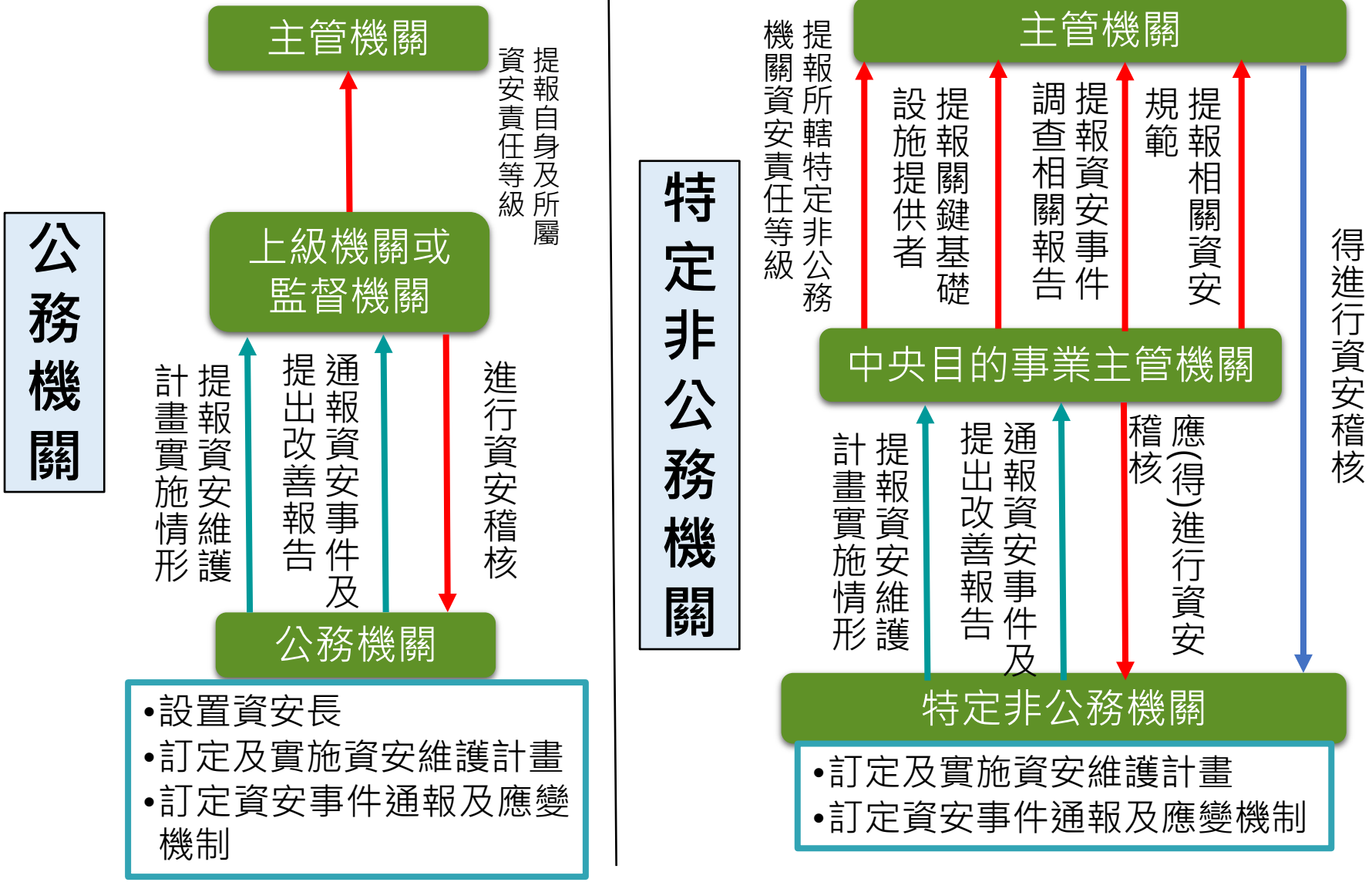
資通安全管理法第3條第8款：

維運或提供關鍵基礎設施全部或一部

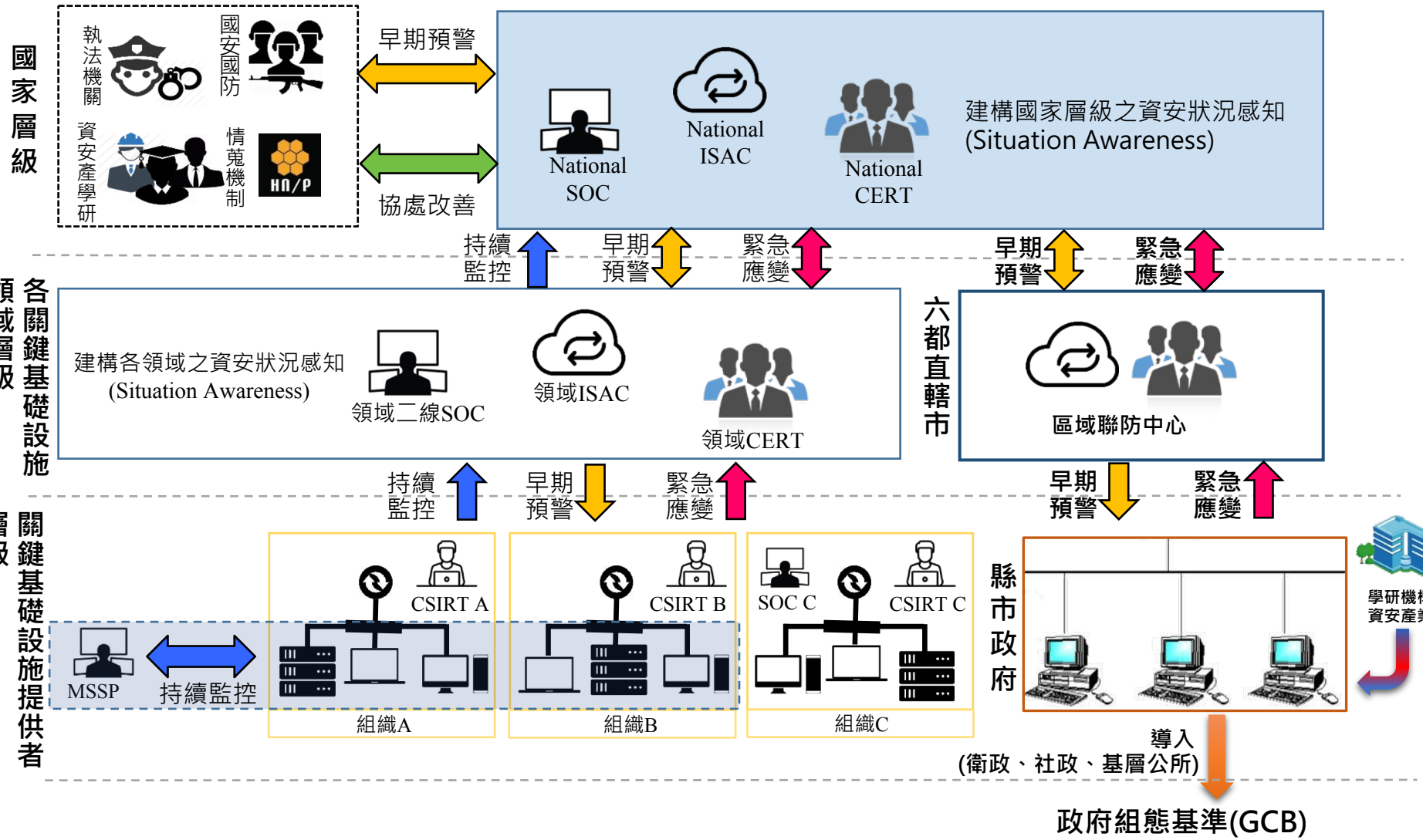
資通安全管理法第16條：
關鍵基礎設施(CI)提供者核定程序



角色與權責


公務機關
主管機關
提報自身及所屬資安責任等級
上級機關或監督機關
提報資安維護計畫實施情形
通報資安事件及提出改善報告
進行資安稽核
公務機關
•設置資安長
•訂定及實施資安維護計畫
•訂定資安事件通報及應變機制
特定非公務機關
主管機關
提報所轄特定非公務機關資安責任等級
提報關鍵基礎設施提供者
提報資安事件調查相關報告
提報相關資安規範
得進行資安稽核
中央目的事業主管機關
提報資安維護計畫實施情形
通報資安事件及提出改善報告
應(得)進行資安稽核
特定非公務機關
•訂定及實施資安維護計畫
•訂定資安事件通報及應變機制

資安聯防整體架構


國家層級
執法機關
國安國防
資安產學研
情蒐機制
早期預警
協處改善
National SOC
National ISAC
National CERT
建構國家層級之資安狀況感知
(Situation Awareness)
持續監控
早期預警
緊急應變
早期預警
緊急應變
各領域關鍵基礎設施領域層級
建構各領域之資安狀況感知
(Situation Awareness)
領域二線SOC
領域ISAC
領域CERT
六都直轄市
區域聯防中心
持續監控
早期預警
緊急應變
早期預警
緊急應變
關鍵基礎設施提供者層級
MSSP
持續監控
CSIRT A
CSIRT B
SOC C
CSIRT C
組織A
組織B
組織C
縣市政府
學研機構
資安產業
導入
(衛政、社政、基層公所)
政府組態基準(GCB)

咦，這些不是資安ABC嗎？

政府該做什麼？

資安為基底推動產業發展以邁向智慧國家

我國現有資安推動政策架構

推動組織	主要推動政策	主要推動計畫	相關部會

行政院國家資通安全會報

國家資通安全發展方案
(106年至109年，行政院資安處)

重點推動項目：

包含基礎環境(如法規、標準)、聯防體系(如協防機制)、產業發展(如產業標準、技術)、人才培育

資安產業發展行動計畫
(107年至114年，行政院資安處)

重點推動項目：

包含人才培育(如設置研訓機構)、技術研發(聚焦利基市場)、場域試煉、國際拓銷

六大核心戰略產業

資安旗艦計畫
(106年至109年，33.3億元)
行政院資安處

前瞻基礎建設資安相關計畫
前瞻1.0(39億元)

- 強化政府基層機關資安防護及區域聯防計畫(34.5億元)
- 強化國家資安基礎建設計畫(4.5億元)

資安卓越產業發展方案
(110年至113年) (66.6億元)

方案計畫包含：

- 前瞻2.0預算35億元，如臺灣資安卓越深耕-資安卓越中心計畫(資安處)及5G及物聯網資安防護-健全電信資安防護設備建置計畫(通傳會)等5項計畫
- 科技預算31.6億元，如資安產業推動暨關鍵基礎設施資安強化旗艦計畫(經濟部)等8項計畫

科會辦
資安處
國發會
經濟部
科技部
衛福部
內政部
通傳會
教育部
交通部
農委會
國防部

一步一腳印，逐步擴大

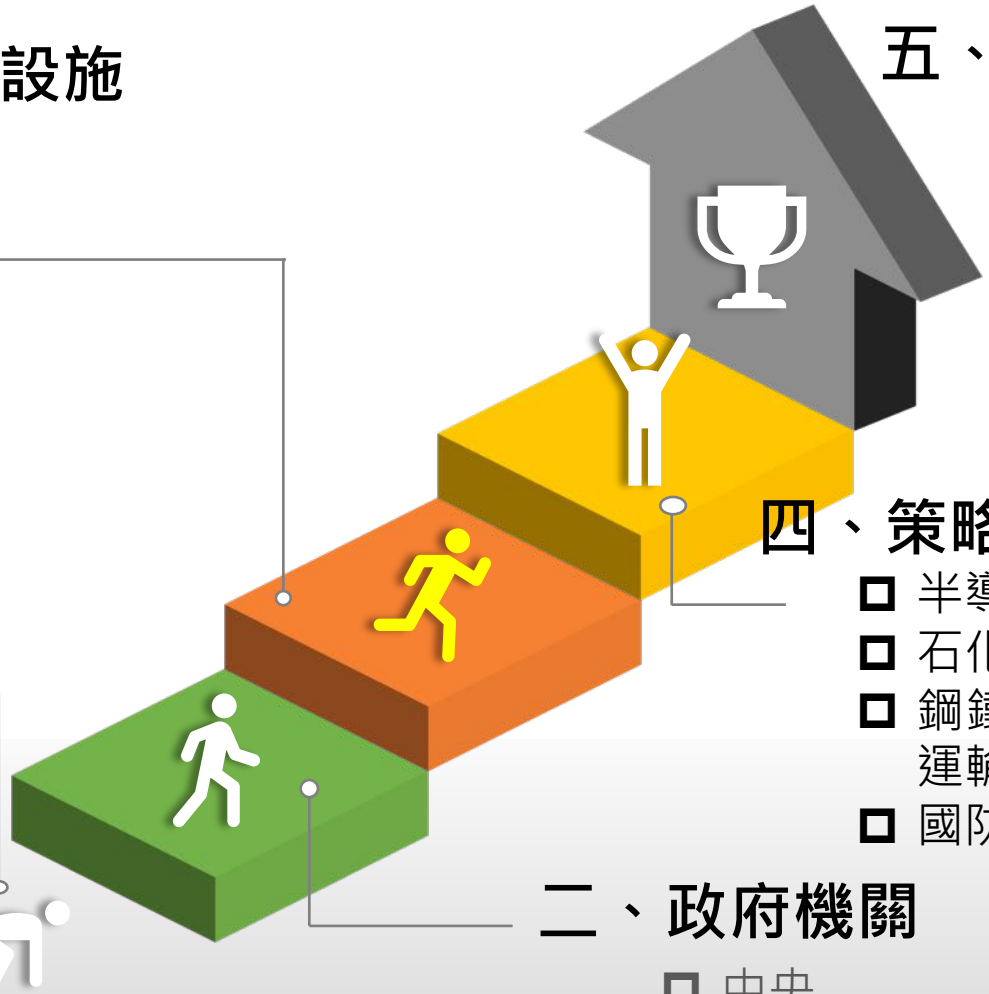
三、關鍵基礎設施

- 水
- 能源
- 通訊傳播
- 交通運輸
- 緊急醫療
- 金融
- 科學園區

五、帶動資安產業發展

四、策略性產業

- 半導體、資通訊
- 石化、食品醫藥
- 鋼鐵、工具機、運輸工具
- 國防、航太



一、資通安全管理法

- 107 年6月6日公布
- 108 年1月1日實施

二、政府機關

- 中央
- 地方
- 國營事業
- 財團法人

SWOT分析

優勢

1、資安為我國重點政策且積極推動
2、訂定資通安全管理法與子法、制定產業標準與檢測規範，完備法律基礎與相關制度配套
3、我國ICT產業供應鏈與工控電腦產品出口優勢
4、我國資訊相關人才素質佳，高階駭客人才藏富於民

劣勢

1、資安法規尚難全面擴及，企業及國民資安意識仍待提升
2、國家整體資安聯防機制仍待深廣化
3、國內資安產業規模較小、產值較低
4、欠缺前瞻研究、實戰及關鍵基礎設施等資安人才

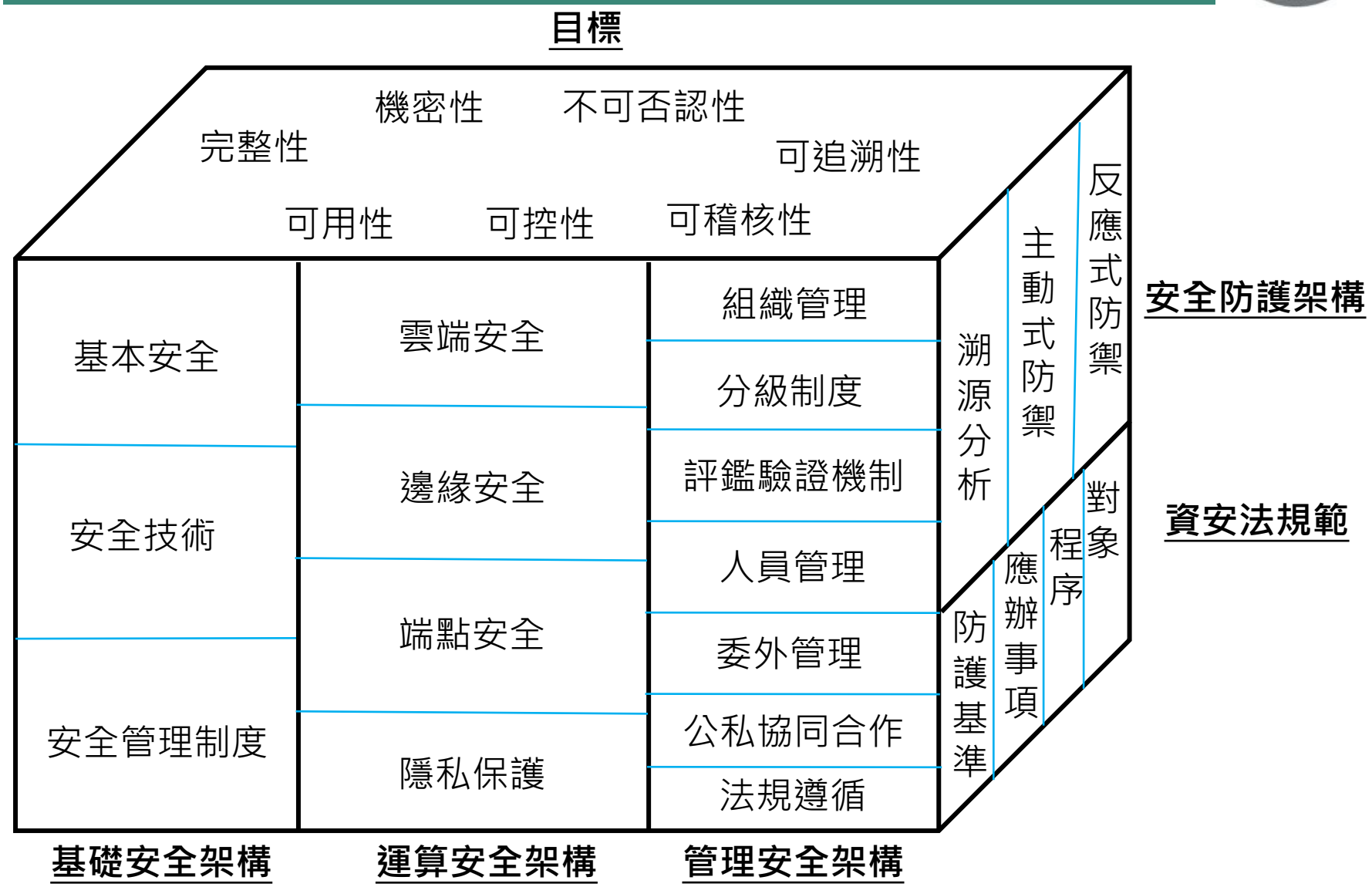
機會

1、我國具有全球重要的資安戰略位置
2、網路犯罪偵查及資安防禦機制等已具一定能量，提升國際合作意願
3、政府資通訊環境逐步集中，有助強化防護
4、5G、物聯網(IoT)、AI及產業創新等資安防護需求日益提升

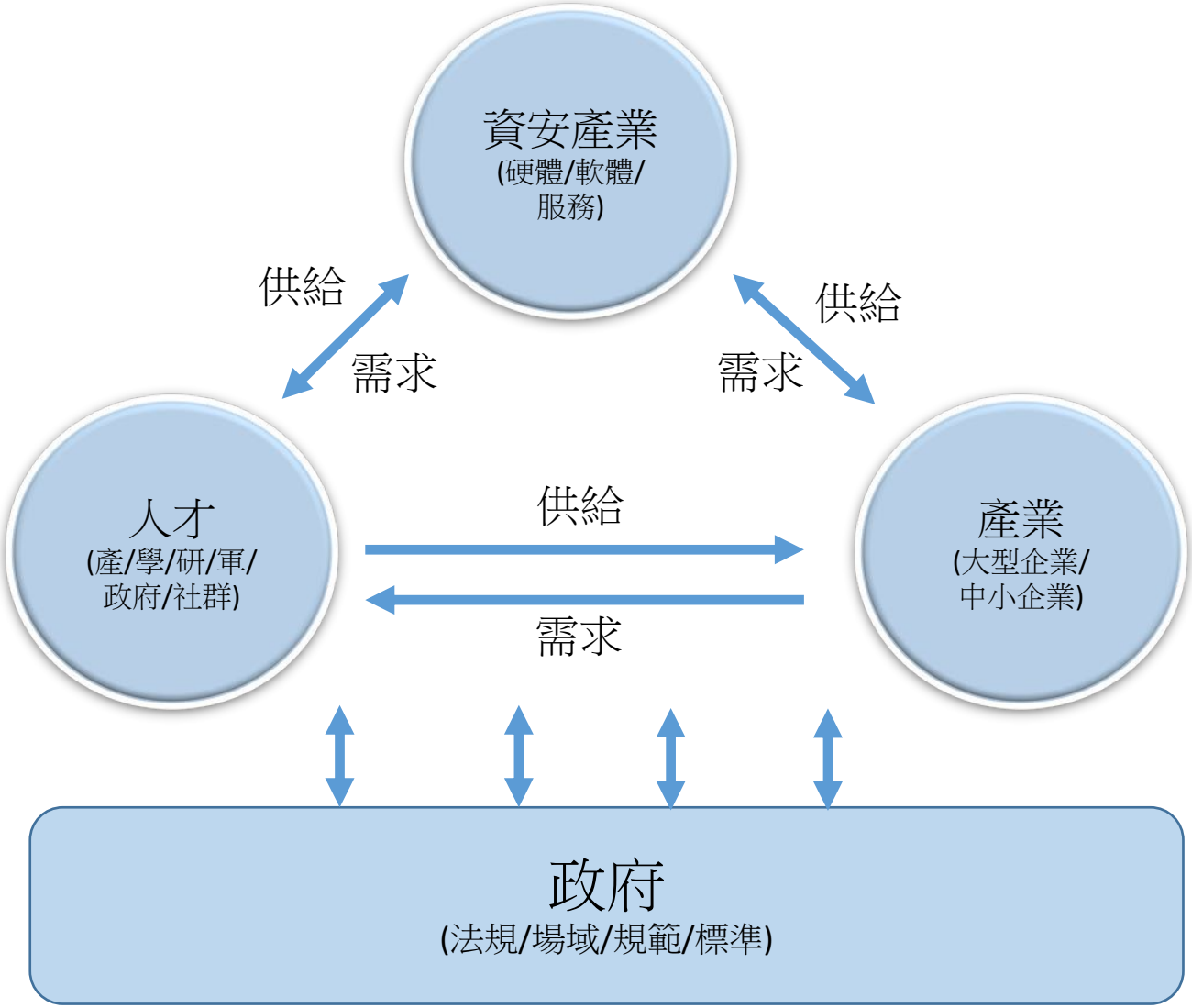
威脅

1、政經情勢特殊，面臨國家級組織駭客威脅
2、新型態資安威脅不斷推陳出新，主動防禦機制仍有不足
3、關鍵基礎設施及供應鏈資安風險日益增加，缺乏公私協同合作機制
4、我國資安業者面臨國際大廠強大競爭壓力

資通安全治理架構
(Cyber Security Governance Framework)



建構資安生態系


資安產業
(硬體/軟體/
服務)
供給
需求
供給
需求
人才
(產/學/研/軍/
政府/社群)
供給
需求
產業
(大型企業/
中小企業)
政府
(法規/場域/規範/標準)

資通安全實施架構

核心理念

實施步驟

具體措施

風險管理

事前

- 界定範圍
- 訂定資安維護計畫
- 採取防護措施
- 資料蒐集分析

事中

- 事件偵測
- 事件通報應變
- 外部稽核及演練

事後

- 復原
- 改善計畫
- 專案查核

國家資通安全發展方案

以風險管理為核心的資安防護

- 蒐集網路流量資訊
- 分析樣態

- 監控網路流量
- 掌握攻擊潛勢

- 數位鑑識
- 追查來源
- 落實改善

- 即時通報
- 應變聯防
- 損害控制

整體防護網

外部情蒐

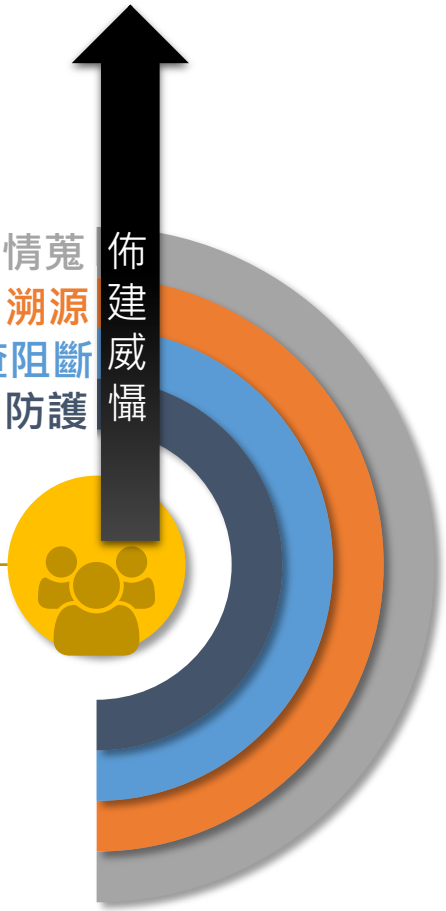
威脅溯源

事件追查阻斷

防護支援

各部會及政府機關

人才培育/資安產業協同合作



提升主動防禦能量

網路攻擊狙殺鏈(Cyber Kill Chain)

偵查
(Reconnaissance)
研究、識別及選擇目標，可以在網際網路上搜尋相關資訊，或是利用工具掃描或探測目標環境。

武裝
(Weaponization)
針對特定的安全漏洞，設計遠端存取木馬程式，包裹在可遞送的資料中，多數以自動化工具產生，且利用常見資料檔案進行偽裝。

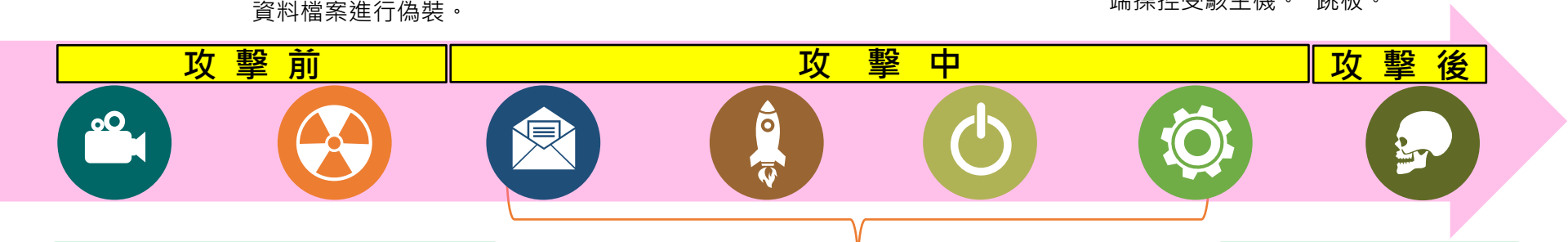
遞送
(Delivery)
設法將惡意程式傳送到目標環境，如電子郵件附件、網站及可移動的USB媒體等遞送管道。

攻擊
(Exploitation)
惡意程式遞送到目標主機後，將觸發內部的程式碼，以應用程式或作業系統的安全弱點為目標，開始進行攻擊。

安裝
(Installation)
於受駭主機安裝遠端存取的木馬或後門程式，而攻擊者可繼續隱藏於受駭環境中。

發令與控制
(Command and Control)
受駭主機須向外連結網際網路上的控制伺服器，以建立控制通道，攻擊者便可利用此通道遠端操控受駭主機。

採取行動
(Actions on Objectives)
攻擊者開始採取行動，如竊取資料、破壞資料的完整性與可用性、或是做為入侵其他系統的跳板。



加強資安整備

- 強化漏洞修補
- 完善備援機制
- 加強資料庫防護

精進縱深防禦

- 完善黑名單防護部署
- 精進資安監控防護
- 落實權限控管

及時應變處理

- 阻斷APT竊密
- 完善系統紀錄

有一個長期的規劃嗎？

國家資通安全發展方案(110年至113年)

願景

打造堅韌安全之智慧國家

目標

- 成為亞太資安研訓樞紐
- 建構主動防禦基礎網路
- 公私協力共創網安環境

推動策略

吸納全球高階人才 培植自主創研能量	推動公私協同治理 提升關鍵設施韌性	善用智慧前瞻科技 主動抵禦潛在威脅	建構安全智慧聯網 提升民間防護能量

具體措施

1. 擴增高教資安師資員額與教學資源 2. 挹注資源投入高等資安科研 3. 培育頂尖資安實戰及跨域人才	1. 建立各領域公私協同治理運作機制 2. 增強人員資安意識與能力建構 3. 公私合作深化平時情資交流與應變演練	1. 賡續推動政府資訊(安)集中共享 2. 擴大國際參與及深化跨國情資分享 3. 制敵機先阻絕攻擊於邊境 4. 提升科技偵查能量防制新型網路犯罪	1. 輔導企業強化數位轉型之資安防護能量 2. 強化供應鏈安全管理 3. 建構安全智慧聯網

資安產業將在5+2產業創新的既有基礎上，配合六大核心戰略產業之「資安卓越產業」規劃持續推動

策略一：吸納全球高階人才培植自主創研能量

成為亞太高階資安人才及技術創新基地

- 擴增高教資安教學資源
  - 擴增資安師資員額
  - 大學區網中心場域
  - 政府開放場域
- 設立資安卓越中心
  - 關鍵核心前瞻研究
  - 深耕學術資安研究
  - 跨國交流合作研究
- 培育資安實戰跨域人才
  - 培育在學資安人才
  - 培訓在職資安人才
  - 研訓頂尖實戰人才

策略二：推動公私協同治理提升關鍵設施韌性

行政院資通安全處

1. 賡續推動資通安全管理法
2. 建立模擬場域，作為實證應處能力及進行教學訓練
3. 建構工控領域資安治理成熟度
4. 推動國家層級資安風險評估

辦理關鍵基礎設施跨領域(或跨國)攻防演練

中央目的事業主管機關

1. 定期稽核所屬關鍵基礎設施提供者
2. 精進關鍵基礎設施資安聯防機制(情資分享、通報應變、資安監控)

定期於場域進行公私聯合攻防演練

關鍵基礎設施提供者

1. 設置資安長並強化人員資安專業能力
2. 落實資安防護基準

策略三：善用智慧前瞻科技主動抵禦潛在威脅

藉由網路攻擊狙殺鏈(Cyber Kill Chain)，制定各個階段之主動防禦作為

偵查 (Reconnaissance)

武裝 (Weaponization)

遞送 (Delivery)

攻擊 (Exploitation)

安裝 (Installation)

發令與控制 (Command and Control)

採取行動 (Actions on Objectives)

推動政府大內網及資安防護向上集中

整合國內外情資來源，並深化國際合作

建立資訊系統弱點之主動發掘、通報及修補機制

應用新興技術淬鍊有效情報，發展主動式防禦前瞻研究及技術應用

完善政府網際服務網防禦深廣度

提升科技偵查能量防制新型網路犯罪

強化新型網路犯罪偵查能量

提升資安事件溯源追蹤能力

加強跨境網路犯罪偵查機制

策略四：建構安全智慧聯網提升民間防護能量

政府機關

- 提升委外供應鏈風險管理
- 強化資通訊晶片產品安全性

- 協助企業提升資安防護能量
- 健全通訊網路安全
- 推動物聯網合規驗證

- 提升民眾資安意識

民間企業

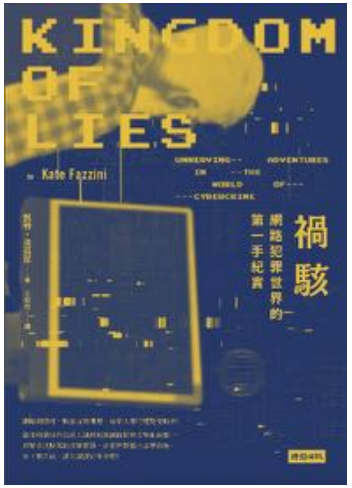
提供安全網路及物聯網設備

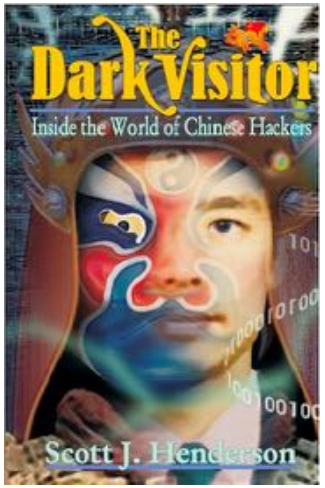
社群個人

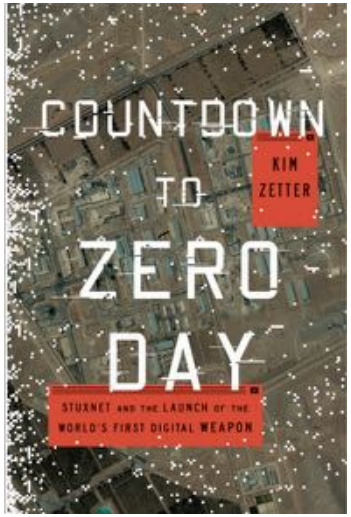
資安是持續精進的風險管理

近期資安參考書籍(1/3)


沙蟲駭客
SANDWORM
安迪・格林伯格
ANDY GREENBERG


KINGDOM OF LIES
Kate Fazzini
禍駭
網路犯罪世界的第一手紀實


The Dark Visitor
Inside the World of Chinese Hackers
Scott J. Henderson

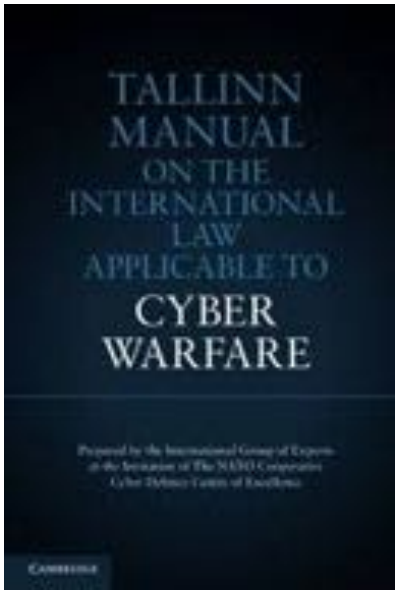

COUNTDOWN TO ZERO DAY
KIM ZETTER
STUXNET AND THE LAUNCH OF THE WORLD'S FIRST DIGITAL WEAPON


資訊科技犯罪
資安戰爭開打！
從心理測驗、交友軟體、廣告信＆假新聞到選舉操控，駭客如何入侵你的真實生活
「今晚你將身敗名裂…」
誰如何傷免於難？
知識是捍衛自己的第一步

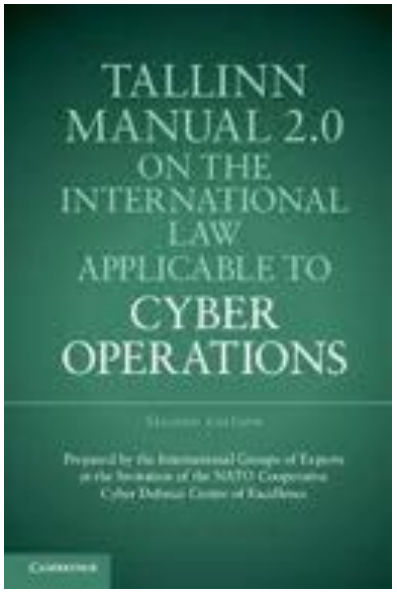

THIS IS HOW THEY TELL ME THE WORLD ENDS
NICOLE PERLROTH
零時差攻擊

近期資安參考書籍(2/3)


建立安全數位世界的第一本書
物聯網
生存指南
5G世界的安全守則
CLICK HERE TO
KILL EVERYBODY
Security and Survival in
a Hyper-connected World
OK
Bruce Schneier


TALLINN
MANUAL
ON THE
INTERNATIONAL
LAW
APPLICABLE TO
CYBER
WARFARE


黑 暗 網 路
匿名地下社會的第一手臥底調查


TALLINN
MANUAL 2.0
ON THE
INTERNATIONAL
LAW
APPLICABLE TO
CYBER
OPERATIONS

近期資安參考書籍(3/3)


無聲的入侵
中國因素——在——澳洲
中國對澳洲的經濟很重要，但是，
澳洲的主權值多少？
SILENT INVASION
CHINA's Influence——in——AUSTRALIA


David E. Sanger
資訊戰爭
THE PERFECT WEAPON
War, Sabotage, and Fear in the Cyber Age


隱形戰
中國如何在美國菁英沉睡時
悄悄奪取世界霸權
STEALTH WAR