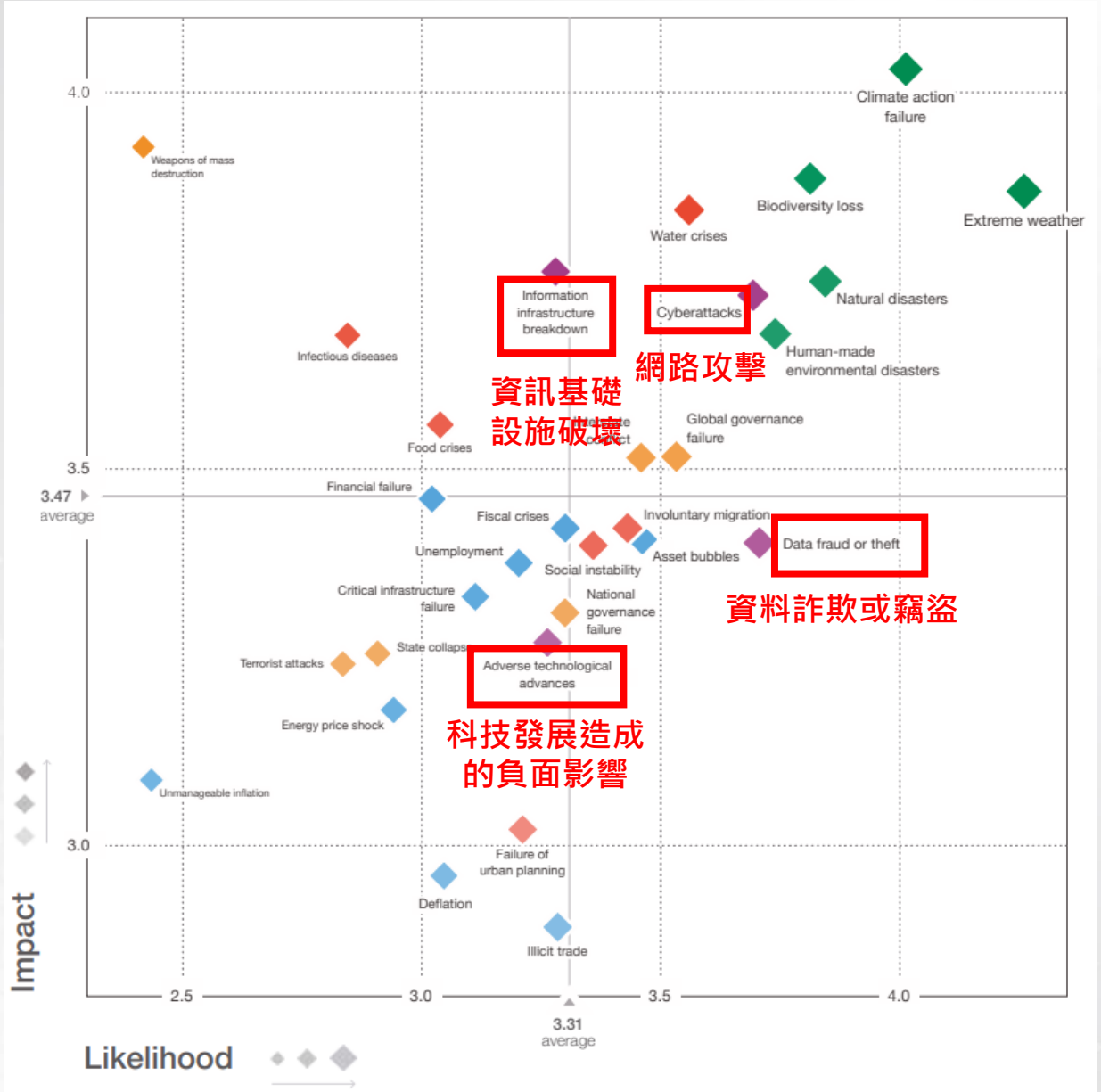
CREATING THE
FUTURE
創 新 · 包 容 · 永 續

安心社會與智慧生活
資通安全

陳俊良教授

行政院 第十一次 全國科學技術會議
Executive Yuan 11th National Science and Technology Conference

世界經濟論壇(WEF) 2020年全球風險報告-資訊安全風險甚鉅



10大影響風險

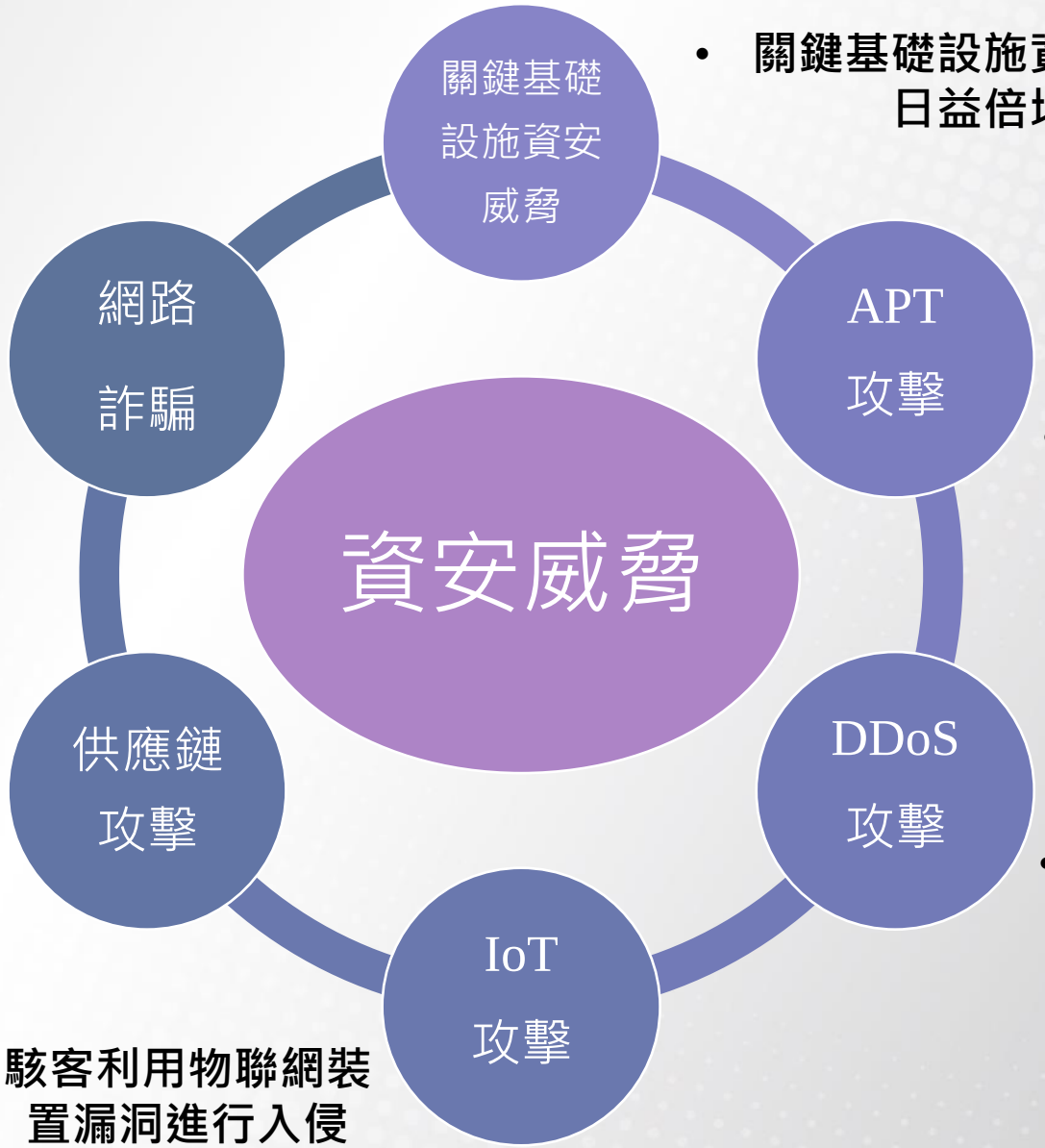
1. 緩解氣候變化與適應失敗
2. 大規模殺傷性武器
3. 生物多樣性喪失
4. 極端氣候
5. 水資源危機
6. 資訊基礎設施破壞(2019年排名第8)
7. 重大自然災害
8. 網路攻擊(2019年排名第7)
9. 人為環境災害
10. 傳染病傳播

10大可能風險

1. 極端氣候
2. 緩解氣候變化與適應失敗
3. 重大自然災害
4. 生物多樣性喪失
5. 人為環境災害
6. 資料詐欺或竊盜(2019年排名第4)
7. 網路攻擊(2019年排名第5)
8. 水資源危機
9. 全球治理失敗
10. 資產泡沫化

Source: The Global Risks Report 2020 15th edition, World Economics Forum

全球面臨的重大資安威脅



- 關鍵基礎設施資安威脅日益倍增
- 駭客利用利用COVID-19冠狀病毒全球大爆發之疫情進行詐騙
- 組織型駭客透過APT攻擊進行資料竊取、加密勒索
- 駭客透過供應鏈攻擊進行滲透到機關、企業內部
- 駭客透過DDoS攻擊癱瘓政府或企業網路與系統運作
- 駭客利用物聯網裝置漏洞進行入侵

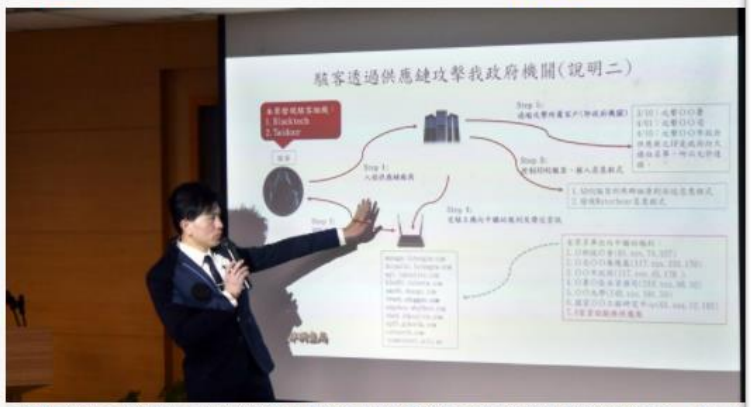
駭客組織透過供應鏈(委外廠商)攻擊政府及企業

- 攻擊型態趨於多元，駭客透過**供應鏈缺口**，進而滲透至企業或機關內部，加強內部資訊安全管理問題刻不容緩，安全防護亦需涵蓋VPN網路

調查局首度揭露國內政府委外廠商成資安破口的現況，近期至少10個公家單位與4家資訊服務供應商遇害

調查局歸納近來偵辦數起臺灣政府機關遭駭案件，在今日（19日）發出警示，需重視委外資訊服務供應商遭中國駭客組織攻擊的現況，近期已有市政府、水資源局等至少10個單位，以及4家以上資訊服務供應商遇害。

文/ 羅正漢 | 2020-08-19 發表



調查局資安工作站副主任劉家榮說明中國駭客如何從臺灣政府委外的資訊服務供應商下手，侵入多

影：羅正漢）

中國駭客組織對我國資訊供應鏈發動攻擊

□ *發布日期 -1802-undefined-undefined 11:03:20undefined 更新日期 -1802-undefined-undefined 08:54:01undefined* □ **公共事務室**

調查局近來偵辦數起我政府機關遭駭案件，調查過程中發現中國駭客組織Blacktech與Taidoor，已長期滲透國內政府機關及其資訊服務供應商，尤其是承接政府機關重要資訊系統之開發及維運，故成為駭客主要攻擊目標，作為跳板攻擊政府機關，試圖竊取機敏資訊及民眾個人資料。為全面清查中國駭客組織利用供應鏈在臺灣網路攻擊活動及遏止我國政府機關持續受駭，調查局成立專案小組積極偵辦。

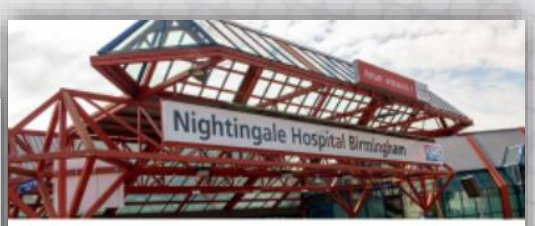
法務部調查局

調查局近來偵辦數起我政府機關遭駭案件，調查過程中發現中國駭客組織Blacktech與Taidoor，已長期滲透國內政府機關及其資訊服務供應商，尤其是承接政府標案之資訊服務供應商，因其負責政府機關重要資訊系統之開發及維運，故成為駭客主要攻擊目標，作為跳板攻擊政府機關，試圖竊取機敏資訊及民眾個人資料。為全面清查中國駭客組織利用供應鏈在臺灣網路攻擊活動及遏止我國政府機關持續受駭，調查局成立專案小組積極偵辦。

調查發現，中國駭客組織深知政府機關為求便利，常提供遠端連線桌面、VPN登入等機制，提供委外資訊服務廠商進行遠端操作與維運，由於國內廠商大多缺乏資安意識與吝於投入資安防護設備，亦未配置資安人員，故形成資安破口，以Blacktech駭客組織為例，該集團主要活動於東南亞地區，駭客先鎖定國內存在尚未修補之CVE漏洞的網路路由器設備，因多數民眾未對設備做韌體更新或修改預設設定，故遭駭客利用此CVE弱點取得該路由器控制權作為惡意程式中繼站，並以另一途徑攻擊國內資訊服務供應商或政府機關之對外服務網站、破解員工VPN帳號密碼及寄送帶有惡意程式之釣魚郵件等，成功滲透內部網路後，利用模組化惡意程式進行橫向移動，本局經分析惡意程式為Waterbear後門程式，受感染電腦會向中繼站報到並以加密連線的方式傳送竊取資訊；另外，駭客為能以多途徑方式持續取得受駭單位內部網路控制權，亦在受駭單位內部伺服器安裝VPN連線軟體，如SoftEtherVPN，其亦可以被利用來對外向其他單位進行攻擊或存取網頁型後門(Webshell)進行竊資。

Fintech獨角獸Dave發生750萬用戶資訊外洩事件，起因竟是過去合作的服務中介廠商遭駭客入侵

Dave.com前服務供應商Waydev遭駭，間接導致Dave.com的用戶資料流入駭客



政府 | 委外 | 外包 | 供應鏈攻擊

英國政府外包商被駭，洩露10萬員工個資

Interserve公司的人事系統資料庫遭入侵，除了波及自家員工個資，其客戶包含英國國防單位、地鐵局及醫院單位，也陷

資料來源：法務部、iThome

國內外層出不窮的目標式勒索攻擊

1. 力X:半導體封測廠湖口廠區遭勒索軟體攻擊，公司對外網站尚未復原。(2020/05)
2. 中X、台X化:遭海外駭客集團勒索攻擊 另有10家遭鎖定。(2020/05)
3. GarXXX: 證實遭俄羅斯駭客集團Evil Group所操控的WastedLocker勒索軟體攻擊造成全球服務停擺。(2020/07)
4. 仁X電腦:疑似遭到勒索軟體攻擊。(2020/11)
5. 研X電腦:工業電腦大廠科技傳出遭到網路攻擊。(2020/11)
6. 巴西最高法院:遭RansomExx毒手而暫時開庭。(2020/11)

資料來源：iThome

案例說明
(台灣中X遭駭客攻擊之手法及途徑)

圖片來源：調查局

透過IoT設備發動DDoS攻擊持續增加

- 2020 DDoS攻擊頻率持續上升
- IoT設備漏洞易於被利用進行攻擊，且數量大幅增加，成DDoS攻擊來源主力
- Cloudflare：2020.7 Mirai殭屍網路病毒感染Moobot IoT設備發起DDoS攻擊，峰值流量高達654 Gbps(來源IP達18,705)

資料來源：中華電信


【漏洞預警】可取國際(icatch)DVR攝影主機遭網路惡意入侵，對外進行DDoS攻擊，煩請儘速確認並進行韌體更新。

上一則公告 下一則公告

張貼者 資訊組長

張貼日期：2020-01-16 15:51:34 點閱：1717

教育機構ANA通報平台

發佈編號 TACERT-ANA-2020011603010808 發佈時間 2020-01-16 15:34:06

事故類型 ANA-漏洞預警 發現時間 2020-01-16 15:34:06

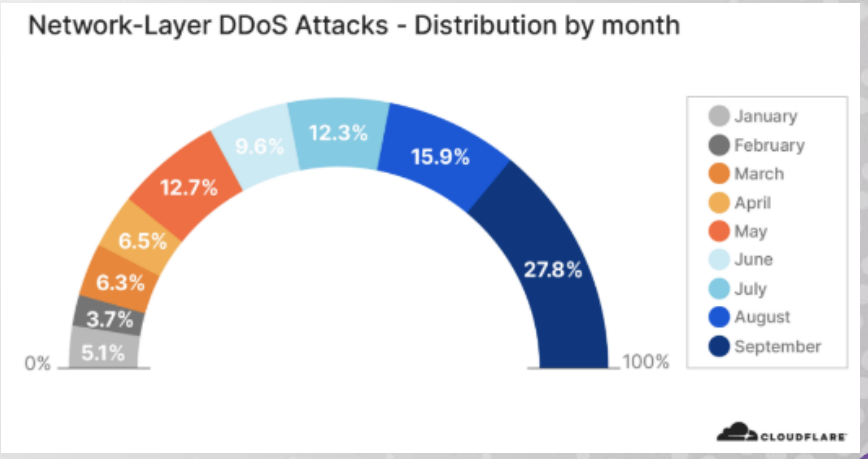
影響等級 低

[主旨說明:]【漏洞預警】可取國際(icatch)DVR攝影主機遭網路惡意入侵，對外進行DDoS攻擊，煩請儘速確認並進行韌體更新。

[內容說明:]

近日可取國際(icatch)DVR攝影主機遭網路惡意入侵，對外進行DDoS攻擊，遭入侵設備會被重設網路介面設定，將連線設定PPPoE改成DHCP模式，造成使用者連線無法連線錄影主機。

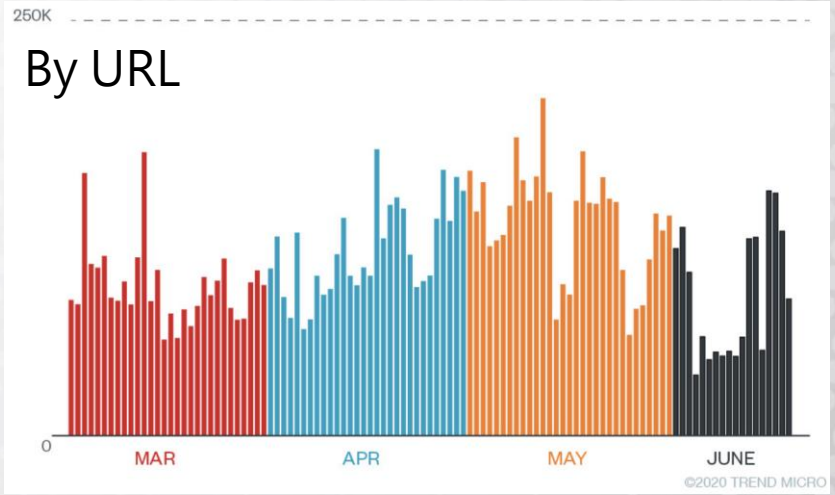
資料來源：https://icatch99.blogspot.com/2019/11/icatch-dvr.html?m=1

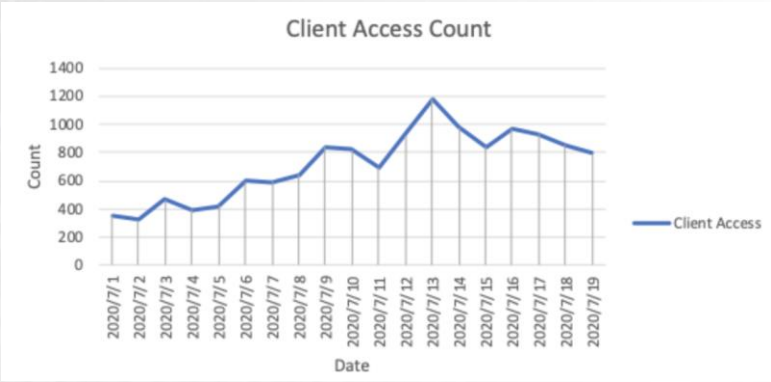


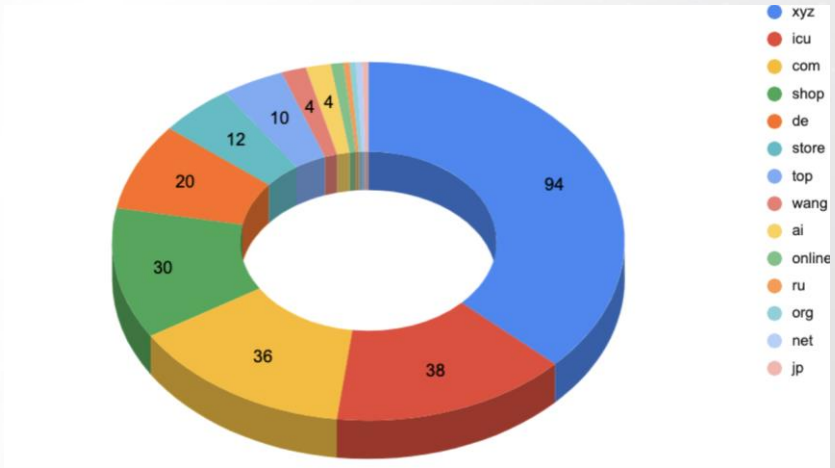
來源: Cloudflare Network-Layer DDoS Attack Trends for Q3 2020

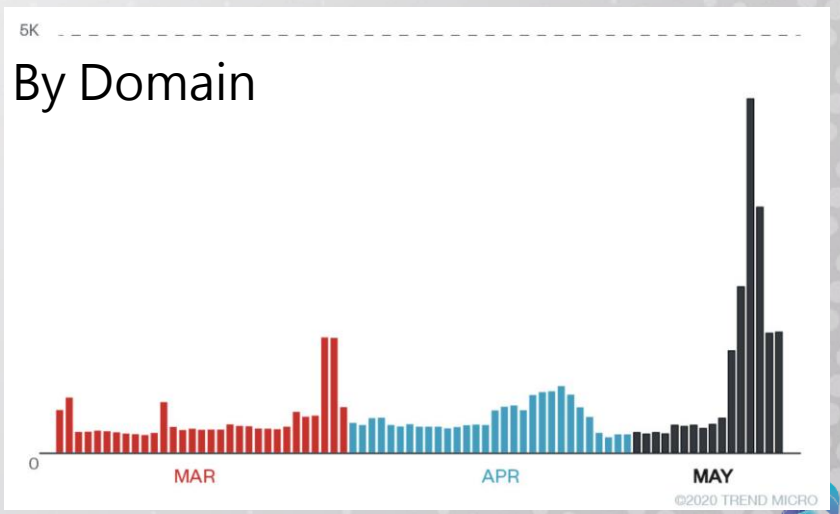
全球線上購物或網路詐騙大幅提升

- 2020 新型冠狀病毒全球大爆發
- 全球為了因應疫情的影響及預防，進而實施遠距教學及工作，因而導致許多人只能透過電子設備來生活或工作，進而大幅提升大眾對網路的需求。
- Trendmicro：2020.7 購物詐騙平均每天有300~1200人在網路商場被欺詐，且這些所連結的購物網站分佈在不同的頂級域（TLD）。









來源: TrendMicro -国内ユーザを狙うネット通販詐欺 2020

資料來源：趨勢科技

資料來源：https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/online-dating-websites-lure-japanese-customers-to-scams

面對資安風險的因應策略

- 建立管理制度，例如：選擇美國NIST網路安全框架（Cybersecurity Framework，CSF）為資訊安全的基準(baseline)， IPDRR
- 建立資安縱深防禦架構，做好網路出入口安全防護，以及持續性的資安防護與安全評估

功能	辨識 Identify	保護 Protect	偵測 Detect	回應 Respond	復原 Recover
類別	• 資產管理 • 營運環境 • 治理 • 風險評估 • 風險管理策略	• 存取控制 • 意識與教育訓練 • 資料安全 • 資訊保護與程序 • 維護 • 防護技術	• 異常與事件 • 持續性的安全監控 • 檢測流程	• 回應計畫 • 溝通 • 分析 • 緩解 • 改善	• 復原計畫 • 改善 • 溝通

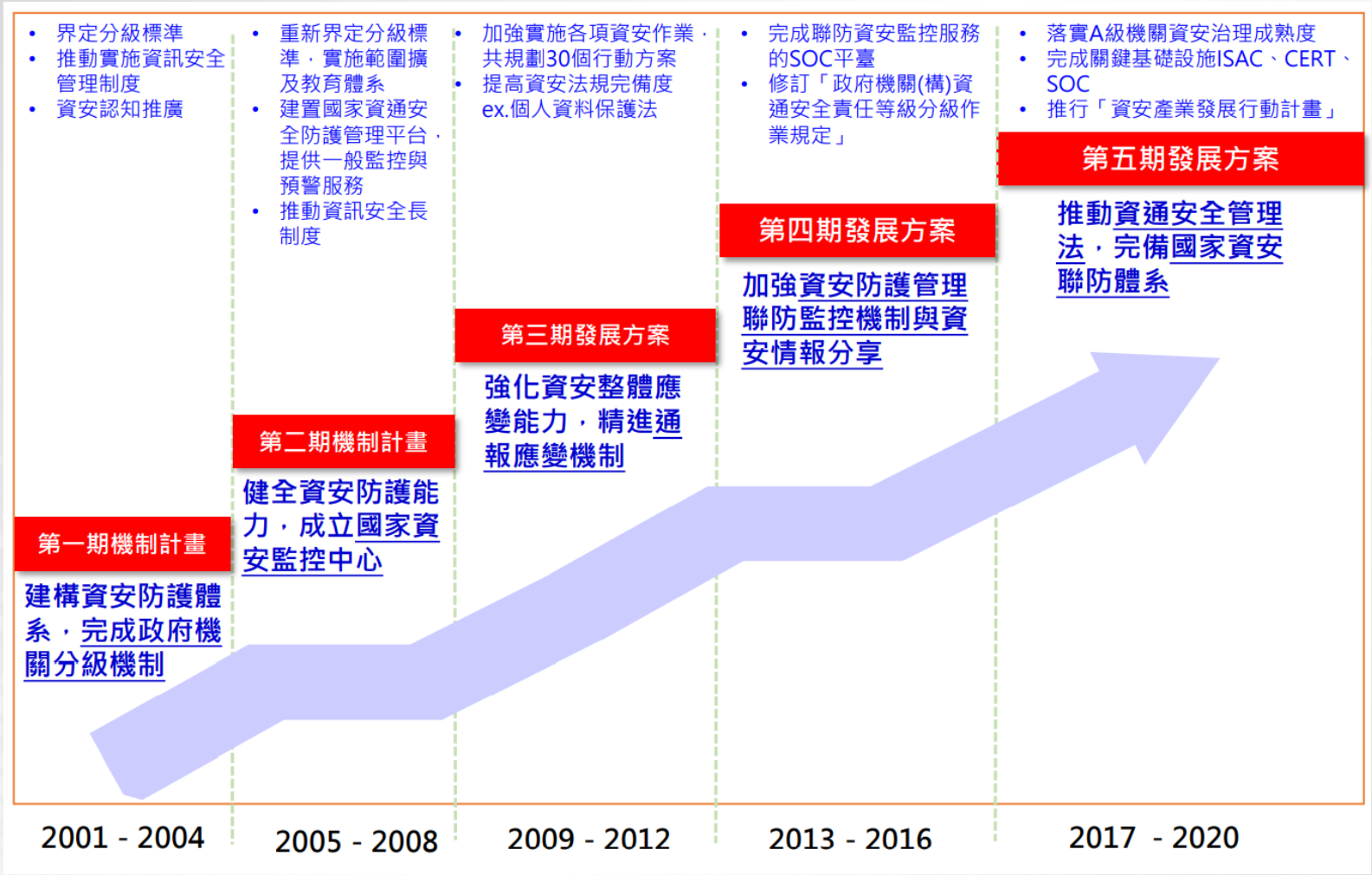
1. 決定實施範圍與優先順序
2. 確認組織目標與方向
3. 建立現況設定檔
4. 進行風險評鑑
5. 建立目標設定檔
6. 判定、分析和考量各種差異的優先順序
7. 實施行動計劃

資料來源：BSI

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

資料來源：NIST

資安持續強化與精進



資安是持續精進的風險管理

- 持續推動區域聯防機制
- 資安聯防機制持續強化
  - 情資分享(ISAC)
  - 事件通報(CERT)
  - 資安監控(SOC)
- 第六期國家資通安全發展方案

感謝聆聽