由新聞事件探討資訊安全重要議題

國家資通安全會報 技術服務中心

劉培文主任

Feb. 27, 2009

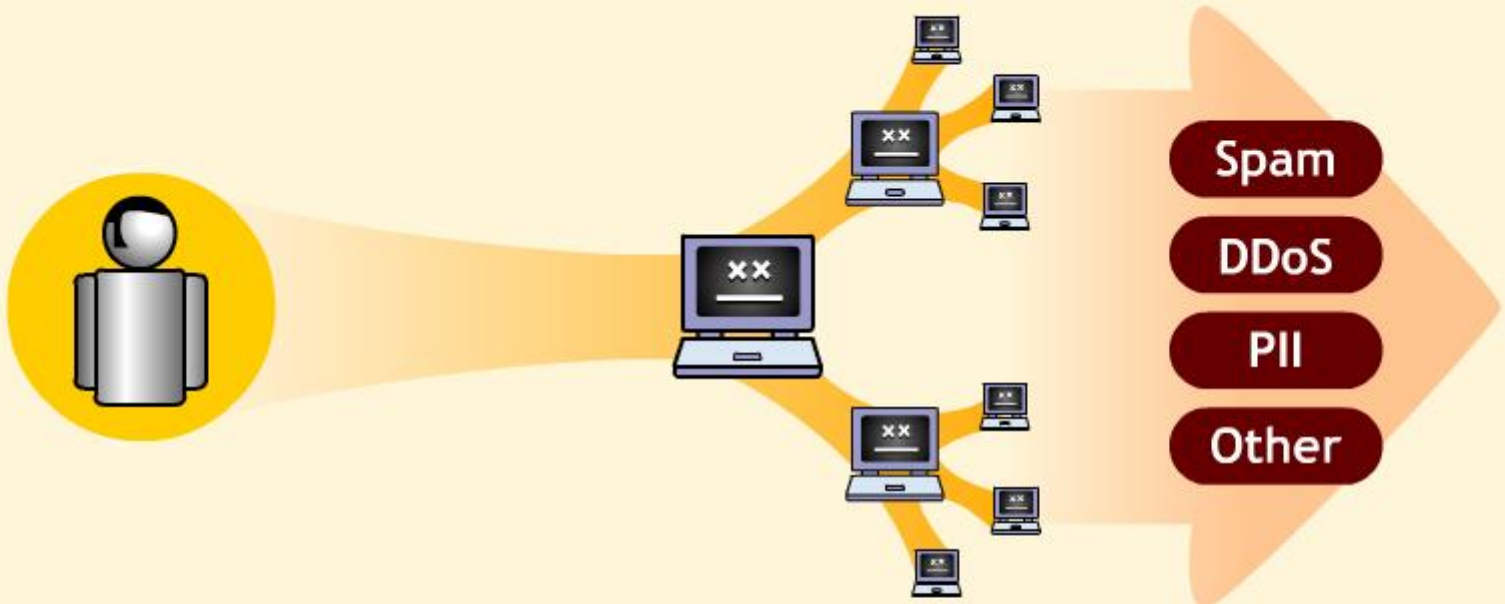
簡報大綱

1. 殭屍電腦網路(*Botnet*)
2. 個資保護(*Personal Identity Protection*)
3. 公務機密保護(*Corporate Espionage*)
4. 關鍵資訊基礎建設保護(*CIIP*)
5. 網路戰爭(*Cyber Warfare*)

簡報大綱

1. 殭屍電腦網路(*Botnet*)
2. 個資保護(*Personal Identity Protection*)
3. 公務機密保護(*Corporate Espionage*)
4. 關鍵資訊基礎建設保護(*CIIP*)
5. 網路戰爭(*Cyber Warfare*)

殭屍電腦網路示意圖



The Infection Spreads

The infection spreads to other machines. A fully-fledged botnet, ready to do the bidding of its herder, can be comprised of hundreds or thousands of machines. Point to a button at the end to see some common uses for botnets.

ILLUSTRATION: ALBERTO MENA; ANIMATION: DAVID SLEIGHT

殭屍電腦網路威脅升級

- 木馬程式Storm Worm自被發現後，八個月內在全球快速傳播，感染兩千萬台個人電腦使其成為僵屍電腦網路大軍
- 根據微軟之研究報告顯示，一個擁有10,000台電腦的Botnet
  - 可以消耗台灣或美國骨幹網路一半的頻寬(4.5Gbps)
  - 足以輕易使一般Web Server中斷服務（VeriSign宣稱針對網域名稱伺服器的阻斷攻擊能夠癱瘓整個網際網路)。

Attack	Requests/bot	Botnet Total	Resource exhausted
Bandwidth flood (uplink)	186 kpbs	1.86 Gbps	T1, T3, OC-3, OC-12
Bandwidth flood (downlink)	450 kbps	4.5 Gbps	T1, T3, OC-3, OC-12, OC-48 (2.488Gbps) **50% of Taiwan/US backbone**
Syn flood	450 SYNs/sec	4.5M SYN/sec	20 tuned server
Static http get (cached)	93/sec	929,000/sec	15 servers
Dynamic http get	93/sec	929,000/sec	310 servers

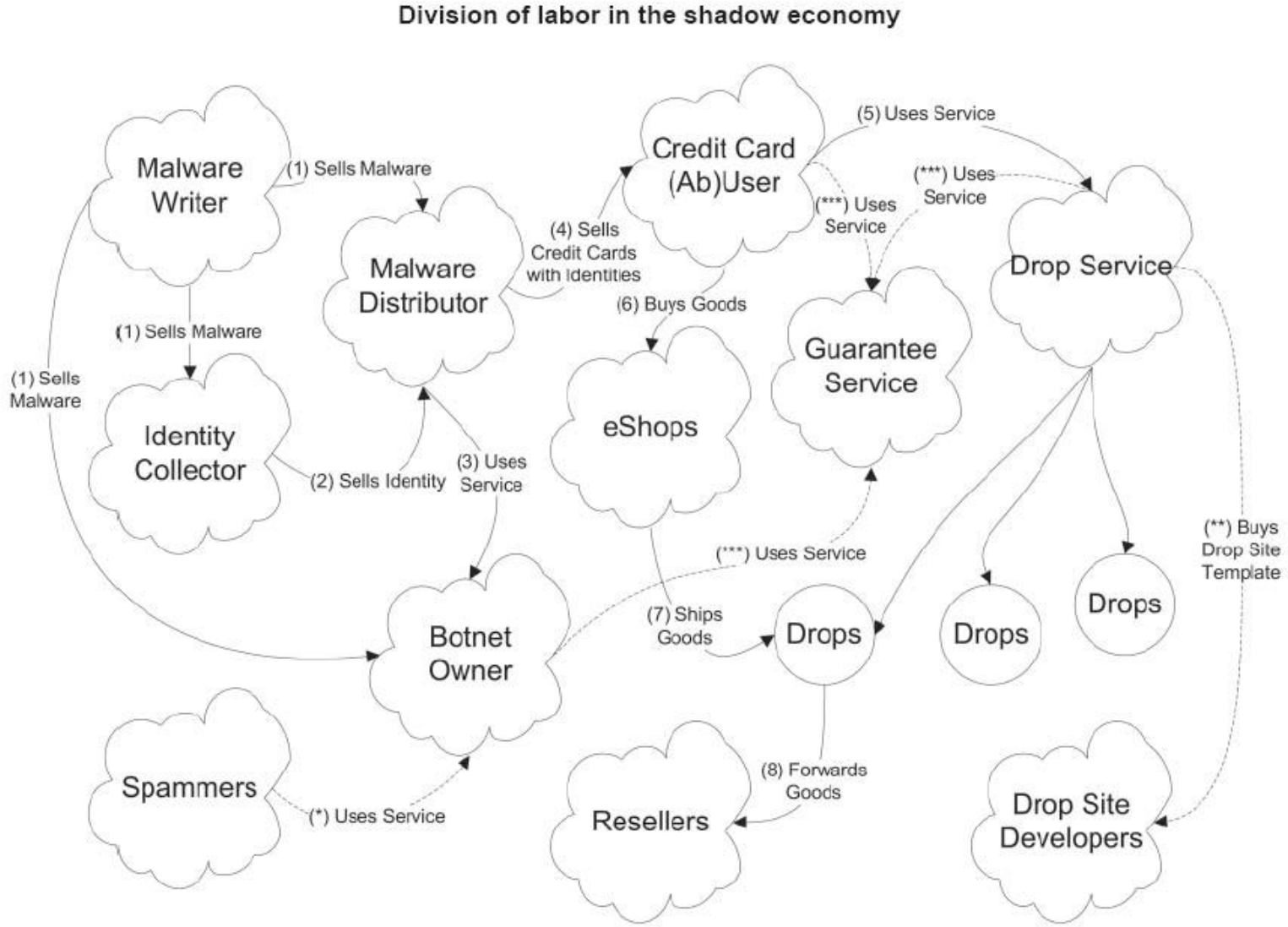
簡報大綱

1. 殭屍電腦網路(Botnet)
2. 個資保護(Personal Identity Protection)
3. 公務機密保護(Corporate Espionage)
4. 關鍵資訊基礎建設保護(CIIP)
5. 網路戰爭(Cyber Warfare)

美國史上最大規模個資竊盜案

- 美國檢方於2008年8月起訴11名國際駭客集團成員，這些駭客近五年共偷了4,100萬筆信用卡及轉帳卡資料
- 此跨國竊盜集團以邁阿密男子岡薩雷茲為首，他開車帶著筆記型電腦尋找商場的無線網路漏洞，駭進商場電腦主機竊取信用卡/轉帳卡帳號密碼，再透過網路賣給美國和歐洲犯罪集團。買家再利用自動提款機盜領受害者帳戶裡的錢
- 美國零售商TJX因客戶卡片遭到盜刷，同意賠償受害的Visa和萬事達卡逾6千萬美元（約18.5億元台幣）

網路地下經濟分工圖



資料來源：*Maksym Schipka, "The Online Shadow Economy: A Billion Dollar Market for Malware Authors", MessageLabs Inc.*

電子商務 vs. 網路地下經濟

- 雲端運算(*Cloud Computing*)
- 電子商務網站
- *Web2.0*
- 電子報/客戶關係管理
- 電子交易機制
  (資訊流/金流)
- 網路促銷
  (購票/王建民商品)

- 殭屍電腦網路(*Botnet*)
- 釣魚網站(*Phishing*)
- 網頁掛馬
- 垃圾郵件(*Spam*)/社交工程
- 惡意程式
  (個資/業務機密)
- 分散式阻斷攻擊
  (*DDoS*)

簡報大綱

1. 殭屍電腦網路(*Botnet*)
2. 個資保護(*Personal Identity Protection*)
3. **公務機密保護(*Corporate Espionage*)**
4. 關鍵資訊基礎建設保護(*CIIP*)
5. 網路戰爭(*Cyber Warfare*)

美眾議員稱中國駭客入侵

- 根據金融時報(*Financial Times*)報導，美國國防部五角大廈於*2007*年*6*月遭到疑似中國之駭客入侵下載政府檔案。美國防部關閉了包括國防部長蓋茲辦公室在內之部分電腦網路。
- 今年*6*月，美國眾議員沃爾夫說，他的辦公室電腦自前年八月開始遭到入侵。眾議員史密斯則指出，他的兩台電腦，分別在前年十二月與去年三月遭到入侵
- 沃爾夫表示，他很早之前就知道駭客入侵，不過美國政界人士卻勸阻他不要公開討論此事。沃爾夫不願透露這些人士的身份

簡報大綱

1. 殭屍電腦網路(*Botnet*)
2. 個資保護(*Personal Identity Protection*)
3. 公務機密保護(*Corporate Espionage*)
4. **關鍵資訊基礎建設保護(*CIIP*)**
5. 網路戰爭(*Cyber Warfare*)

SCADA 網路攻擊破壞概念證明出現

- 2007年3月美國進行了代號 Aurora Generator Test的實驗。由愛達荷國家實驗室複製一座輸電網，並對其SCADA (Supervisory Control And Data Acquisition)系統進行網路入侵測試
- 美國國土安全部在2007年9月底公布了實驗結果
- 駭客成功入侵了輸電網並使一部柴油發電機冒煙進而遭破壞
- 國土安全部羅伯特傑米森：「透過網路發動攻擊，能造成設備的損壞。」
- 如果駭客在網路同步攻擊主要的電力系統，若全美有1/3的電力系統關閉3個月，等同於40到50個大型颶風掃過

簡報大綱

1. 殭屍電腦網路 (*Botnet*)
2. 個資保護 (*Personal Identity Protection*)
3. 公務機密保護 (*Corporate Espionage*)
4. 關鍵資訊基礎建設保護 (*CIIP*)
5. 網路戰爭 (*Cyber Warfare*)

愛沙尼亞衝突事件

- *2007*年*4*月愛沙尼亞政府將一座*1947*年蘇聯時期的二戰紀念「軍人銅像」從首都市中心搬走，因而引發了網路騷亂(*Cyber-riot*)，更有媒體及政客稱此為第一次的網路戰爭(*Cyber Warfare*)
- 愛沙尼亞的媒體、銀行與電子化政府等網路服務遭受了至少*128*次的分散式阻斷式攻擊(*Distributed Denial-of-Service, DDoS*
- 此分散式阻斷攻擊規模雖比不上過去癱瘓*Yahoo*、*Amazon*、*CNN*、*eBay* 等知名網站的攻擊事件，但由於愛沙尼亞之高度*e*化，對該國之影響範圍幾至全民

結論

- 組織型駭客持續覬覦公務及商業機密
  - 以電子郵件社交工程之針對式攻擊為主要手段，透過網路入侵各國政府及其外包廠商，進行網路情搜
- 網際空間電子化服務可用性威脅提升至國家層級
  - 殭屍電腦網路(*Botnet*)已不光被網路罪犯作為網路經濟犯罪工具，更成為國與國對抗，可被租用與徵調的「第五縱隊」

結論

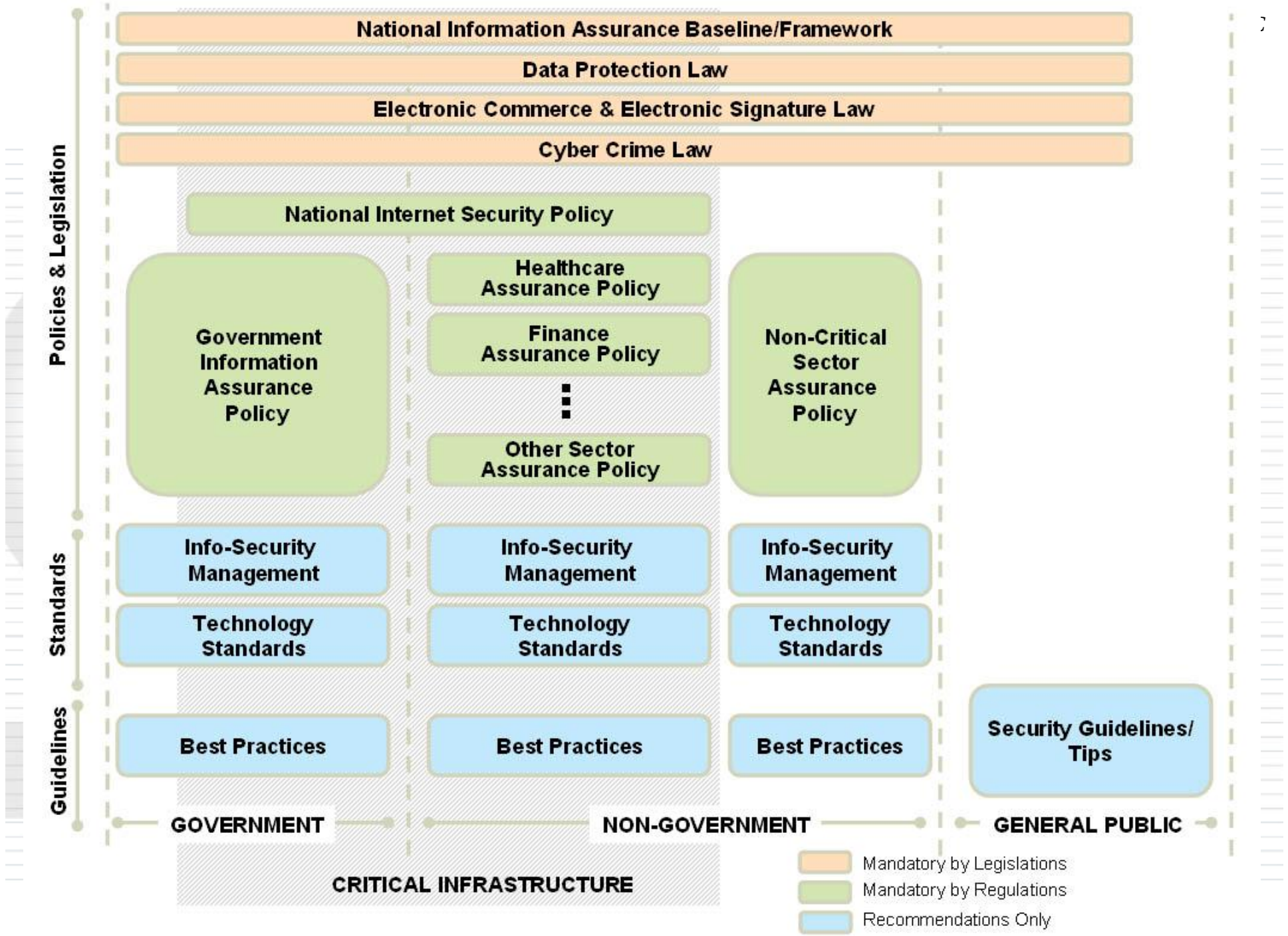
- 關鍵基礎建設透過網際網路遭實體破壞風險倍增
  - 關鍵基礎建設大量使用之管理控制與資料擷取系統(*Supervisor Control And Data Acquisition, SCADA*)其網路攻擊破壞概念證明(*Proof of Concept, POC*)已陸續出現
- 經濟罪犯大量竊取個人隱私
  - 主要利用使用者信任的網站，以「網頁掛馬」大量竊取民眾之隱私資料，輔以「鎖定對象之匿蹤攻擊」進一步進行洗錢或其他經濟犯罪

技術服務中心業務簡介

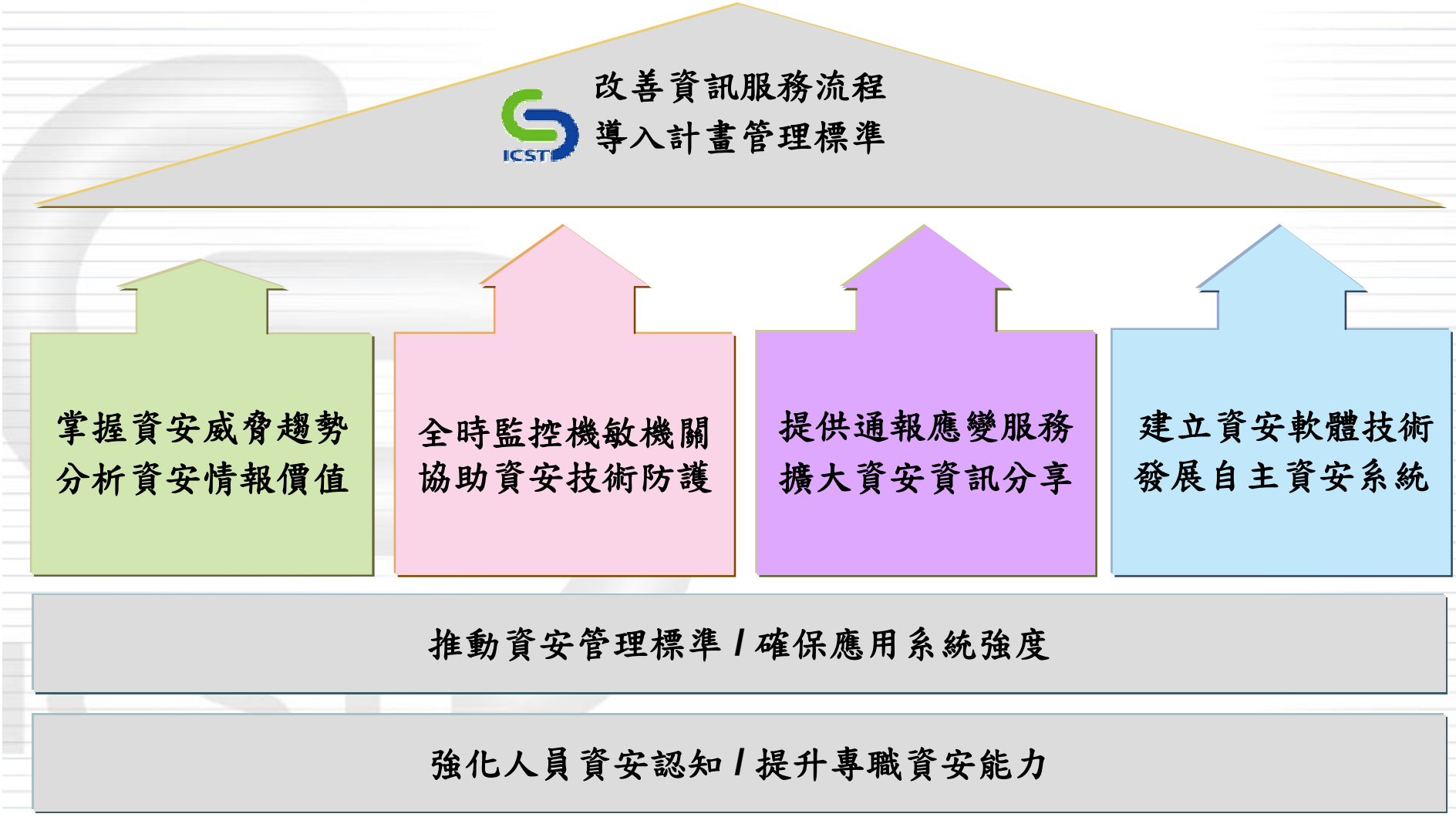
國家資通安全會報 技術服務中心

劉培文主任

Feb. 27, 2009


National Information Assurance Baseline/Framework
Data Protection Law
Electronic Commerce & Electronic Signature Law
Cyber Crime Law
National Internet Security Policy
Government Information Assurance Policy
Healthcare Assurance Policy
Finance Assurance Policy
Other Sector Assurance Policy
Non-Critical Sector Assurance Policy
Info-Security Management
Info-Security Management
Info-Security Management
Technology Standards
Technology Standards
Technology Standards
Best Practices
Best Practices
Best Practices
Security Guidelines/ Tips
Policies & Legislation
Standards
Guidelines
GOVERNMENT
NON-GOVERNMENT
GENERAL PUBLIC
CRITICAL INFRASTRUCTURE
Mandatory by Legislations
Mandatory by Regulations
Recommendations Only

技術服務中心任務


改善資訊服務流程
導入計畫管理標準
掌握資安威脅趨勢
分析資安情報價值
全時監控機敏機關
協助資安技術防護
提供通報應變服務
擴大資安資訊分享
建立資安軟體技術
發展自主資安系統
推動資安管理標準 / 確保應用系統強度
強化人員資安認知 / 提升專職資安能力

重點工作

資安認知與專業職能

公務員專業職能

- 專業技術研習
- 專業證照/職能課程

公務員認知

- 數位學習教材
- 全省巡迴講習

未來人才培育

- 資安攻防金盾獎
- 資安動畫金像獎

全民認知

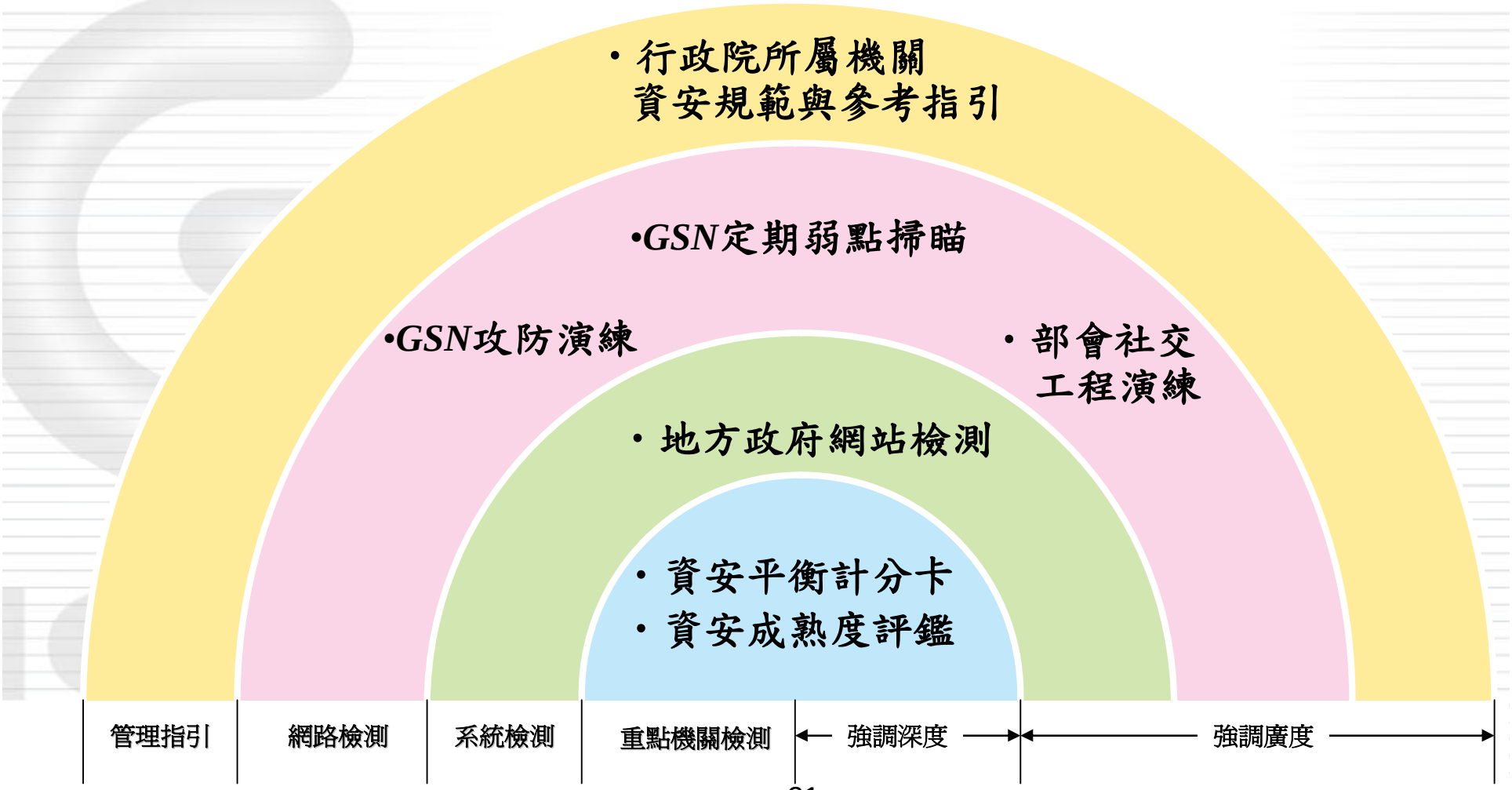
- 資安週系列活動

強調深度

強調廣度

重點工作(續)

Ÿ 資安管理與系統安全



重點工作(續)

Ÿ 威脅情資與通報應變