

新個資法趨勢及企業衝擊分析

資料命脈掌控與洩漏保護策略分享



A Smarter Planet



Smarter Security & Resilience

A Smarter Planet

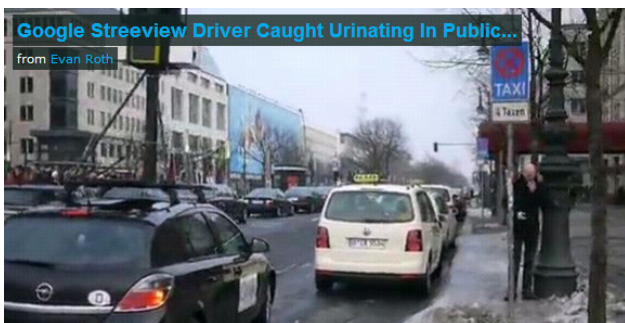
Welcome to the
Decade of Smart

Google地圖「街景服務」的社會衝擊與隱私爭議

Google街景車的駕駛被拍到在公共場所尿尿

自從Google Map推出了街景服務後，各地只要出現Google的街景車都會成為眾人的目光焦點，不過在德國的柏林，一位民眾好奇的跟著街景車走但是卻拍到了令人反感的畫面，不知道駕駛是不是憋太久，突然的走下車在路邊的路燈旁公然的小起便來，真是一點公德心都沒有...而且當路過的民眾發現街景車停下來都紛紛的拿起相機和手機拍攝，只見駕駛尿完之後還非常優閒的走回車內，一點都不在乎大家的眼光。

報導來源：<http://funvideo.idv.tw/>



Google maps

「街景服務」：以置身街頭的角度來探索世界



使用「街景服務」

縮放、旋轉和環視世界上各城市的街景照片。



哪裡提供「街景服務」服務？

我們為哪些城市提供「街景服務」服務？我們的街景拍攝車現在在哪些城市收集影像？



幕後秘辛

關於我們的車輛、影像，以及您最忠實的「街景服務」導遊 - 「夾夾人」。



隱私權政策

瞭解 Google 如何保護您的隱私權，以及如何回報不適當的圖片。



圖片來源：自由時報 / 歐新社

報導：街景車收集Wi-Fi資料，Google可能面臨多國政府調查據各地媒體的報導。

德國、捷克、加拿大及美國資料保護機構有意調查Google的街景車透過Wi-Fi收集個人資料的行為。

Google在上周坦承，該公司的街景攝影車不小心蒐集了使用者利用公開Wi-Fi網路所傳遞的資訊，雖然Google已停止個人資料的蒐集行為，並對已蒐集的資訊展開銷毀，但媒體報導，德國、捷克、加拿大及美國資料保護機構有意全面調查Google的行為。

根據英國金融時報的報導，捷克資料保護組織UOOU已在本周對Google的作法展開調查，衍生的罰款可能達48.2萬美元；此外，德國已有網路律師控告Google未經授權蒐集使用者資訊，德國檢察官正在研究是否立案。

USA Today則報導加拿大負責處理隱私權的官員正在尋求其他國家的結盟，以共同討論Google蒐集個人資料的作法。美國消費者保護機構Consumer Watchdog亦在本周要求美國聯邦交易委員會（FTC）立刻進行調查Google的行為。

鼓吹消費者權益的John M. Simpson認為，Google在重演「先做再說，錯了再道歉」的戲碼，有鑑於Google近來涉及的隱私弊病，沒有理由相信Google對其資料蒐集政策的說辭。Simpson表示，FTC應該要詢問Google究竟蒐集了哪些資料、如何處理，以及Google是何時知道的。

今年4月，Google曾經說明Google街景攝影車並未蒐集個人隱私資料，但在德國政府要求Google重新檢視所蒐集的資料後，上周Google坦承該公司攝影車的確意外蒐集到公開Wi-Fi網路上所搭載的個人資料，除了立即宣布停止蒐集相關資料外，亦邀請第三公正單位見證已蒐集資料的銷毀。

Google周一（5/17）表示，Google攝影車在愛爾蘭所蒐集的隱私資訊已在上周末經第三方見證下全部銷毀，Google正繼續與其他國家的資料保護機構接洽，以儘快銷毀所有的資料。

不過，Simpson形容由Google邀請第三方來監督的作法就像是在棒球決賽中欽點裁判，有失公允，相關的調查應該要由具備真正制裁能力的監管機關執行。

報導來源：iThome



Smarter Security and Resilience
*An intelligent approach to risk
management reveals opportunities
for innovation*

Agenda :

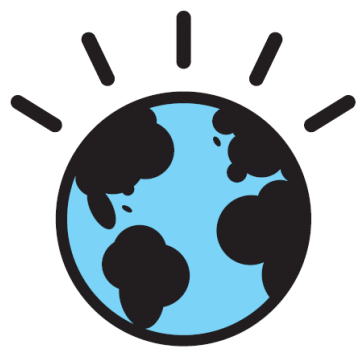
- 個資洩漏之統計資料及研究分析
- 新版個資法之內容定義及企業衝擊分析
- 資料命脈掌控與洩漏保護策略





個資洩漏之統計資料及研究分析

- 主要事件來源分析
- 個資洩漏損失分析



國內的個資外洩問題不斷且常成為媒體焦點，且跡象顯示內部人員行為和外界的入侵同等重要

出賣考生個資 博暉判賠349萬

*Source: 聯合報

【聯合報／記者呂開端 BLOG／桃園報導】

2009.06.07 02:29 am

台中市博暉公司承包去年國中基測業務，以50萬元販賣考生資料3萬4千多筆給補教業者，主辦基測的國立桃園高中向博暉訴請每洩漏一人罰100元的懲罰性賠償，桃園地院昨天判博暉應賠償349萬餘元。

桃園地院調查，博暉公司標到97年國中基測事務，負責基測的電腦報名、建立各國中集體報名和**盜賣資料**、加密電子檔等，還與主辦的國立桃園高級中學簽定「**盜賣資料**」的契約。

桃園法院指出，博暉公司負責人因積欠債務，有意利用考生資料牟利，透過中間人物色買考生個人資料的補習班，隨後以50萬元的價碼，將台中地區、彰化、南投等地的3萬4965名考生的基本資料和測驗分數燒成光碟後，賣給五家補教業者。

超離譜 網售東森購物 8千筆個資

業者屢出包 卡號全都露 每筆5毛

2009年06月11日蘋果日報

新聞快訊 列印(37) 轉寄(0) 引用(0) 書籤

【郭睿誠、侯柏青／台中報導】八千筆東森購物台消費者個人資料在網路上「全都露」。有民眾周一在網路上宣稱「輸錢賣信用卡資料」，強調是「東森購物流出**內部管控?**」身分證字號等一應俱全。該名業者表示，他經營的「東森購物」有二十多所學校的資料，資料內容包括姓名、地址、電話、生日、身分證字號等。《蘋果》經抽樣訪問確認資料無誤。東森購物接獲《蘋果》查訪後表示已向警方報案；消基會則呼籲民眾慎選其他更安全的交易平台。

*Source: 蘋果日報

老師個資外洩 網站找得到

民視 (2009-05-30 15:55)

轉寄好友 友善列印

Ads by Google

Branding Taiwan 短片競賽 Youtube.com/TaiwanExcellence

發揮你的創意,以5分鐘短片呈現台灣產業風貌,向世界發聲,還有機會拿獎金!

台中縣教育處不久前，彙整各校認輔老師的個人資料，結果100多位老師的個資卻不慎外洩，並且在中國知名網站，都能夠找到這些老師的個資，雖然網站已經把資料刪除，但老師們擔心，會讓有心人惡意使用。幾天前在中國的入口網站，發現有100多位認輔教師的個人資料，全都一覽無遺，原來是台中縣政府教育處，在資料傳輸時出了差錯，教育處承辦人員的疏忽，造成100多位老師的生日、身分證字號和住址等個人資料，在網路上曝光，老師擔心有心人利用個資犯罪。

未知原因

*Source: 新浪網



2009-3-21

*Source: 自由時報

4校長涉賣10萬學生個資

與補習班勾結 中彰廿多校受害

〔彰化小組／綜合報導〕校長為錢，竟然出賣學生！彰化地檢署去年底接獲檢舉，指稱員林鎮大佳補習班涉嫌與多所學校校長、甚至前教育局長勾結，以現金行賄取得學生資料，資料內容包括姓名、地址、電話、生日、身分證字號等。該網表示，上週日檢閱資料來自**盜賣資料**。

彰檢襄閱主任檢察官張慧瓊指出，檢方針對涉案重大的校長與業者展開監聽調查，今年二月初展開搜索約談，在主嫌吳芝庭（卅六歲）經營的大佳補習班搜到大批學生名冊與帳冊，吳芝庭坦承行賄校長，但因牽涉的學校過多，為免吳芝庭串證或湮滅證據，將她收押至今。

個資洩漏的相關統計資訊及研究報告：主要事件來源

個資洩漏事件，最主要可粗
分為下列幾種事件來源：

節點防護不足

- 筆記型電腦或個人電腦的遺失或被竊取
- 遺失或被竊取的儲存媒體

未有整體防禦架構

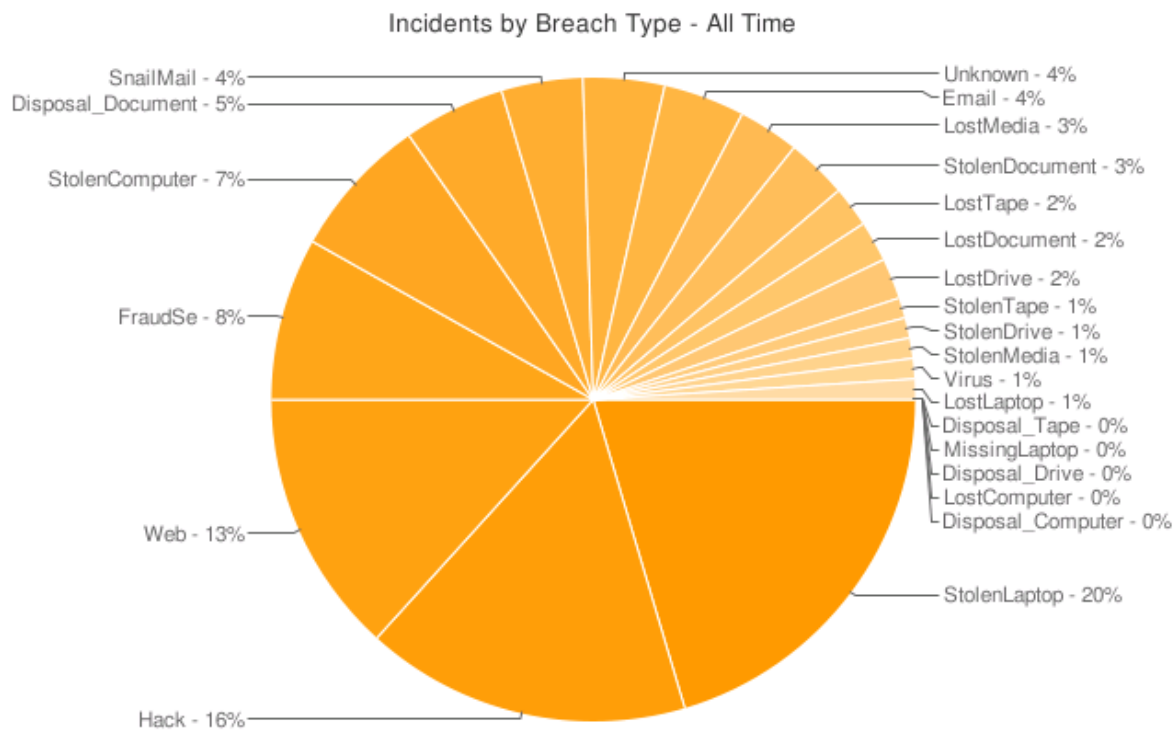
- 外部駭客攻陷Web應用程式或資料庫，抓取個資

缺乏資料運用政策

- 惡意的高權限內部系統管理者或維護廠商

未具備資料外洩處理分析能力

- 惡意的內部使用者



個資洩漏的相關統計資訊及研究報告：個資洩漏損失

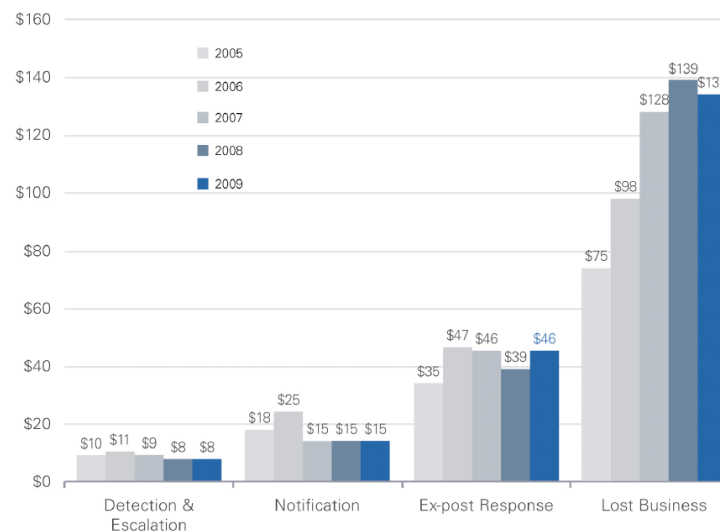
- 大型個資洩漏事件於2009年仍持續發生
(史上第一及第四大個資洩漏事件)

Largest Incidents

RECORDS	DATE	ORGANIZATIONS
130,000,000	2009-01-20	Heartland Payment Systems
94,000,000	2007-01-17	TJX Companies Inc.
90,000,000	1984-06-01	TRW, Sears, Roebuck
76,000,000	2009-10-05	National Archives and Records Administration
40,000,000	2005-06-19	CardSystems, Visa, MasterCard, American Express
30,000,000	2004-06-24	America Online
26,500,000	2006-05-22	U.S. Department of Veterans Affairs
25,000,000	2007-11-20	HM Revenue and Customs, TNT
17,000,000	2008-10-06	T-Mobile, Deutsche Telekom
16,000,000	1986-11-01	Canada Revenue Agency

Source: DataLossDB, Open Source Foundation

- 單筆洩漏之資訊造成企業之直接與潛在損失以2009年之最新估計約為204美金
- 個資或機密資料洩漏造成企業實際的Revenue損失約為3~8%的企業revenue比例
- 企業極可能數年就發生一次大規模的個資或機密資料外洩



Source: 2009 Annual Study: Cost of a Data Breach, Poneman Institute, 2010

個資洩漏之損失除實質貨幣付出外，亦含括商譽之影響

Heartland Payment System遭竊取一億三千萬筆信用卡資訊

“Heartland Payment Systems是美國第六大之信用卡刷卡服務提供商，每月平均處理超過1億筆信用卡交易。於2009年1月20日HPS宣布內部發現遭駭客以惡意軟體竊取交易中之未加密信用卡條碼資訊，共約一億三千萬筆信用卡資訊遭到洩漏”。

影響：該公司股價(HPY)當日暴跌43%，
並造成發卡銀行須回收並重製受到影響之信用卡

TJX Company遭竊取九千四百萬筆客戶資訊

“TJX Company是美國最大的服飾及家用品百貨零售商。於2007年1月17日TJX宣布內部發現遭駭客入侵電腦資訊系統，估計共約九千四百萬筆客戶資訊（含交易及信用資訊）遭到洩漏”。

影響：包括支付公共調查及律師費用、以及與Visa及相關銀行部分之賠償協商方案等實質
付出之貨幣損失約為六千五百萬美金
（不含消費影響、股價損失等其他非直接損失，估計近五億六千萬美金）

Source: DataLossDB, Open Source Foundation

除個人資料之外，營業秘密亦是企業應考量的重點

個人資料

(被動，法律損失或商譽損失)

- 個人資料是指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料；
- 個人資料保護不好，可能造成的是法律賠償與訴訟費用，以及商譽的損失

營業秘密

(主動，直接造成營運損失)

- 營業秘密是指不為公眾所知悉(不公開的)，能為權利人帶來經濟利益，具有實用性並經權利人採取保密措施的技術資訊和經營資訊；
- 營業秘密的洩漏會直接造成企業之營運損失、核心競爭力下降



各行業都有營業秘密資料，如：製程流程與參數、財務資料、員工個人資料、客戶個人資料...。而且從外部入侵或在內部盜取都可能發生

不論個人資料或是營業秘密皆是「資料」保護的範圍及核心

行業別	營業秘密	個人資料
科技及製造業	製程流程與參數、設計資訊、未公開產品規格、軟體原始碼、營運及業務、財務、人事資訊	雇員個人資料
金融行業	交易資訊、未公開營運資訊、業務、財務、人事資訊	雇員個人資料、客戶個人資料、信用卡或帳戶資訊
醫療行業	實驗數據、業務、財務、人事資訊	雇員個人資料、病患個人資料、病歷資訊、健康檢查資訊
教育行業	研究報告、業務、財務、人事資訊	教職員資訊、學生及家長個人資料、學生學習紀錄
政府及軍事	軍事機密資訊、內部調查資料、未公開規劃、稅務資訊、情報資訊	國民、市民資訊、個人稅務及財務資訊、
零售行業 網路商店	交易資訊、未公開營運資訊、業務、財務、人事資訊	會員資訊、信用卡或帳戶資訊



新版個資法之內容定義及 企業衝擊分析

- 新個資法定義、適用性、時程及範圍
- 新個資法對企業之主要影響
- 新個資法對IT之主要影響



個資法最新定義及適用情形

第二條 本法用詞，定義如下：

1. 個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。
2. 個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。
3. 蒐集：指以任何方式取得個人資料。
4. 處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。
5. 利用：指將蒐集之個人資料為處理以外之使用。
6. 國際傳輸：指將個人資料作跨國（境）之處理或利用。
7. 公務機關：指依法行使公權力之中央或地方機關或行政法人。
8. 非公務機關：指前款以外之自然人、法人或其他團體。（原僅規範徵信、醫院、學校、電信業、金融業、證券業、保險業、大眾傳播）
9. 當事人：指個人資料之本人。






新版個資法的實施時程及範圍

- 1995/07/12 立法院三讀通過「電腦處理個人資料保護法」
- 1996/05/01 電腦處理個人資料保護法施行細則發佈實施，規定政府與八大行業（徵信、醫院、學校、電信業、金融業、證券業、保險業、大眾傳播
- 1997 ~ 2010/03 11次修法擴大非公務機關適用產業 (如: 百貨公司業及零售式量販業電腦處理個人資料辦法，無店面零售業 ...)
- 2010/04/27 立法院三讀通過「個人資料保護法」，適用於所有公務、非公務機關及個人(老闆與經手員工)。施行日另訂，預測約為2011年六月開始施行 (於施行細則公佈後)
- 新版個資法包含所有個人資料之蒐集、處理及利用，含紙本資料而非前法案訂定僅針對電腦處理之個人資料，以及如護照號碼、健康檢查資訊...等之前未含括之個資範圍



新版個資法對企業的主要影響簡介

- 公務機關及非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏 
- 非法變更、刪除個人資料致妨害正確性足以損害個人時：五年以下、一百萬以下罰金之之刑責 
- 鼓勵由財團法人或公益團體協助一般受損害之個人提起團體訴訟
- 民事賠償責任上升：賠償上限由原來之兩千萬變成兩億（且若證明事實損害若大於兩億的話則以事實為限）
- 強調非公務機關須免費提供個資當事人拒絕利用其個人資料進行行銷之機制
- 企業非直接向當事人蒐集個人資料，必須在法案實施一年內告知當事人。當事人必須書面同意才能使用
- 企業必須自行舉證沒有違反個資法 
- 故意及非故意都罰：
 - 非故意而產生損害 -> 2年以下有期徒刑、拘役或併科罰金20萬以下
 - 意圖營利 -> 5年以下有期徒刑、拘役或併科罰金100萬以下



面對新個資法「採行適當之安全措施」、「資料之完整性」以及「證明無故意或過失責任」，是免責之主要關鍵



法規要求	個資法所涉及IT議題
應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏	如何強化資料運用與保護架構
非法變更、刪除個人資料致妨害正確性	如何健全節點資料存取及洩漏保管機制
資料外洩損害賠償，非公務機構需證明「無故意或過失責任」，才能免責	如何建立資料外洩風險評估與處理分析能力

無故意或過失責任?
-採行適當措施?
-如何提出證明?

企業主與經辦人員
須負起民事及刑事
責任!!



罰兩億元(以上)!?

如何知道企業流程中哪些環節會使用個人資料?

如何預防個人資料外洩? 如何保留相關稽核紀錄?

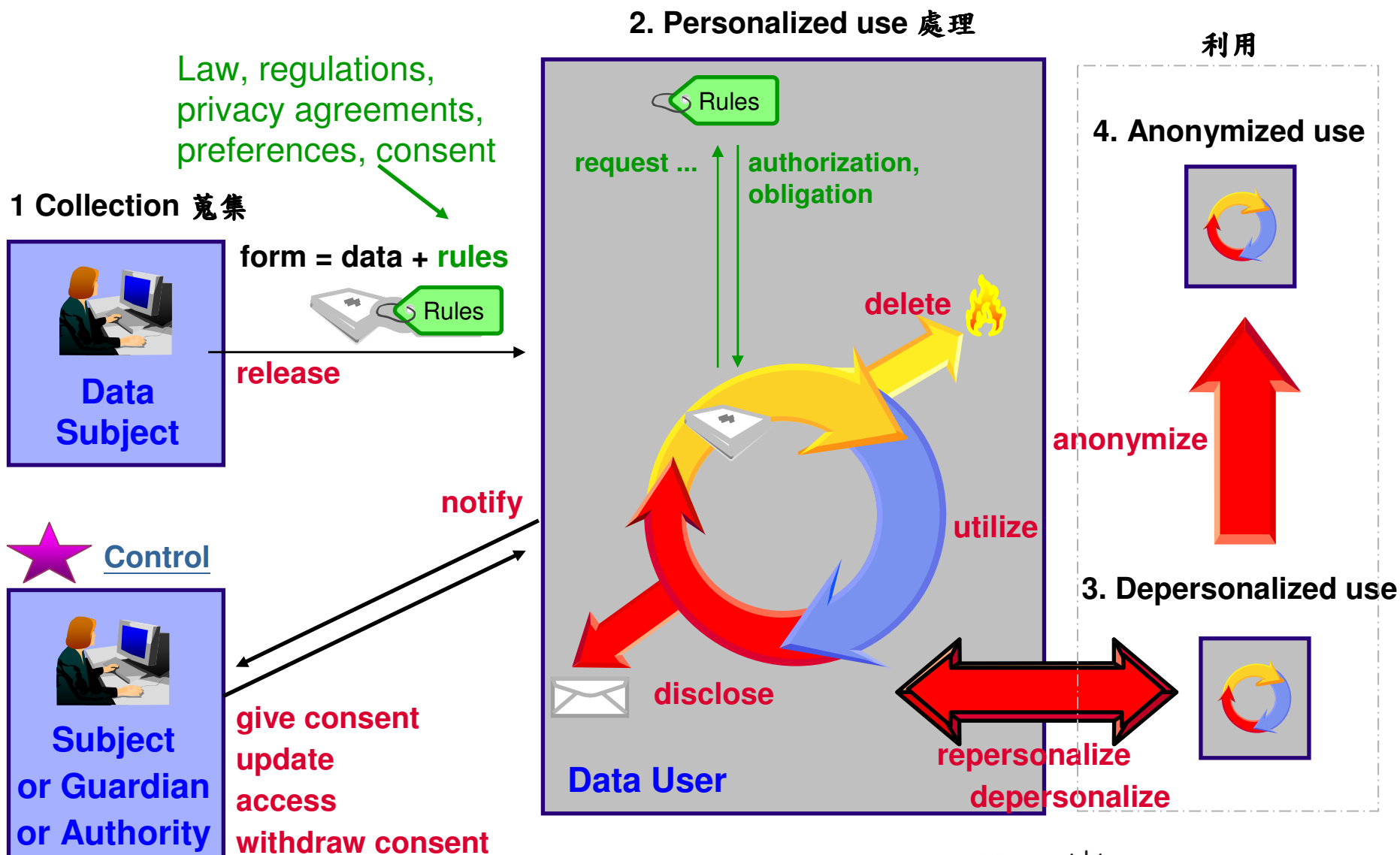


資料命脈掌控與洩漏保護策略

- 整體運行參考架構
- 資料安全整體規劃藍圖建議
- 策略方向及施行



個人資料/營業祕密之生命週期防護架構參考



資料安全的整體架構必須是全面性的考慮：客戶需全面且整體性重新檢閱資料散佈情形、建立資料的資產管理機制、評估各項資料的外洩風險、依據風險高低運用「機制、工具或監控」等方式達到管理目標

一般而言，企業面對個資法可採取的因應措施大致可分為兩大方向：

1. 評估個資外洩的風險
2. 建立符合需求的個人資料保護系統

在評估個資外洩風險時，需瞭解個資外洩主的可能管道：
外部入侵、委外廠商洩漏、內控程序疏失，以及內部人員洩漏等



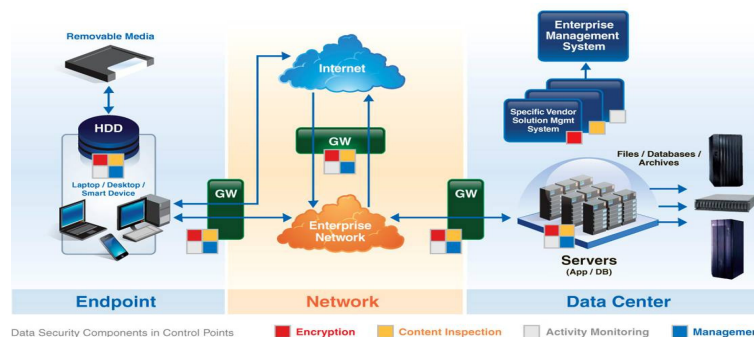
but

如何開始?

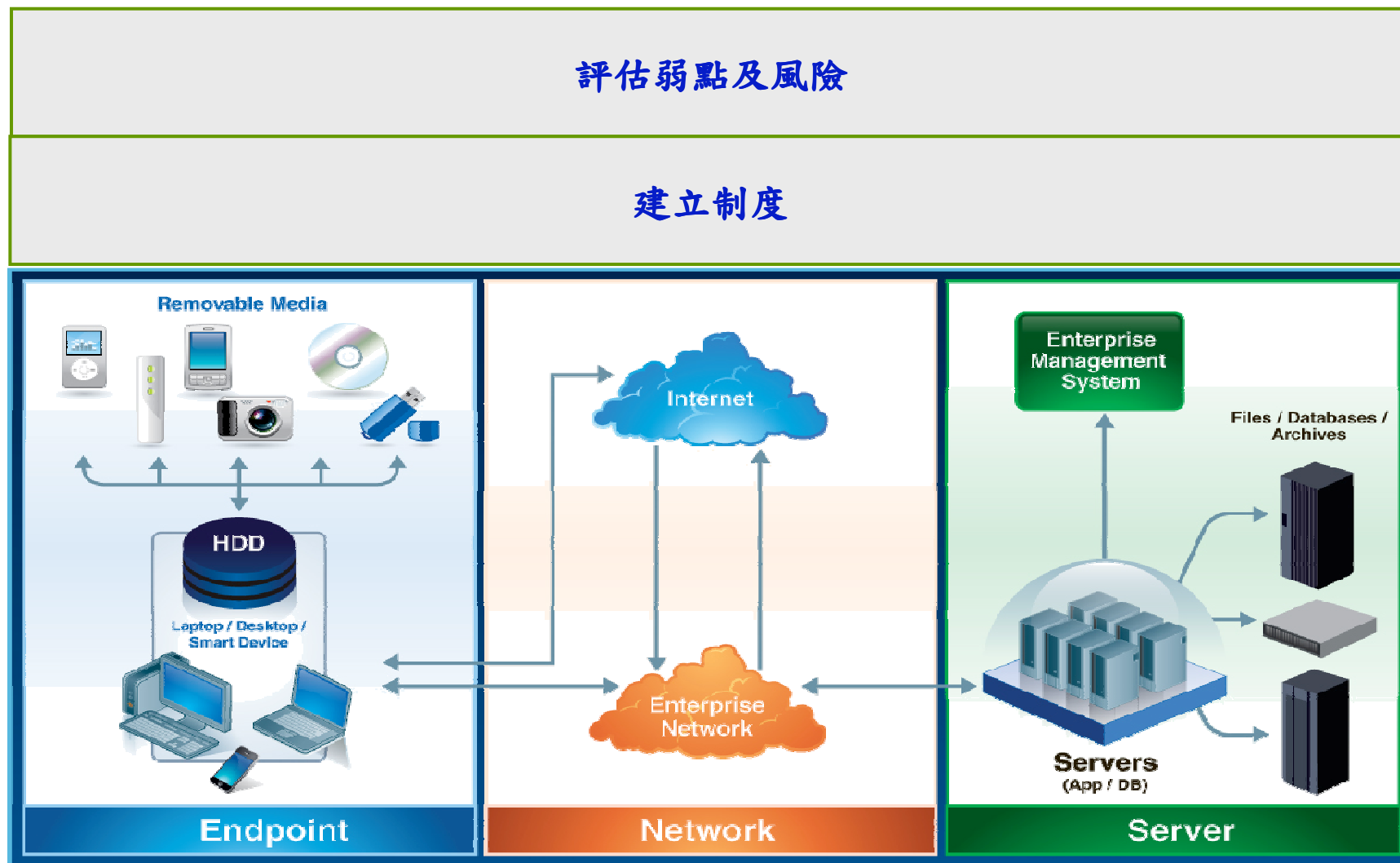
在建立符合規範的個人資料保護系統時，也要先了解個人資料處理的流程：

1. 蒐集階段，要依法進行告知義務並取得書面同意
2. 其次是處理，採取適當保護措施避免個人資料被竊取、竄改或毀損
3. 利用階段，客戶資料必須依蒐集時的特定目的範圍內才可使用，（如果要在範圍外使用，必須另外取得書面同意。）
4. 最後是銷毀，這也是最容易被企業忽略的階段，如果蒐集資料時的目的消失了，或期限屆滿，企業必須將資料完全銷毀。

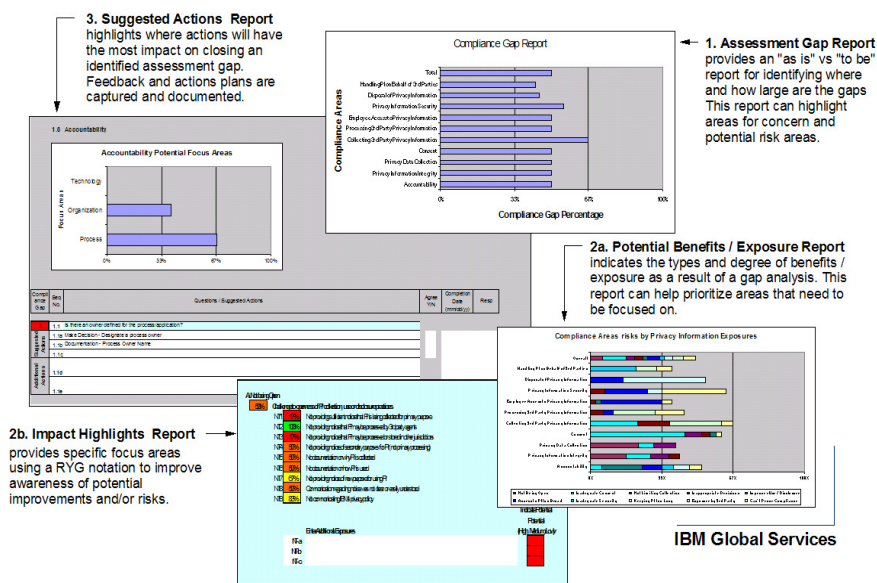
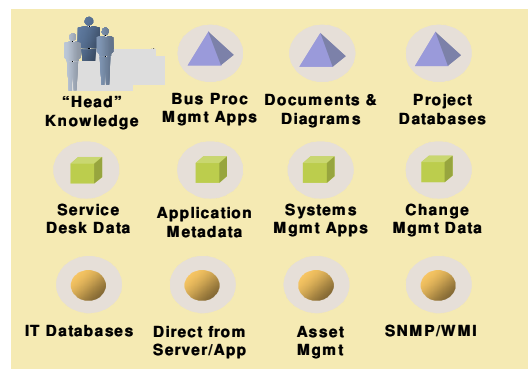
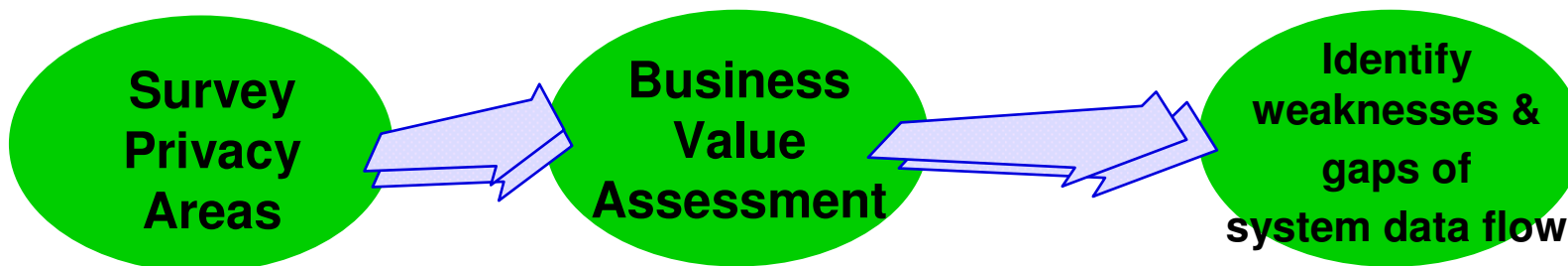
也必須考量個人資料處理的含括面向：
移動式儲存媒體、個人處理節點、
網路、應用系統、資料庫、
伺服器以及儲存體等



企業資料安全牽涉到資訊安全防護的各個層面，包含端點、網路、伺服器端；而經由評估自己的弱點及風險來採取相對的因應措施才能切中目標

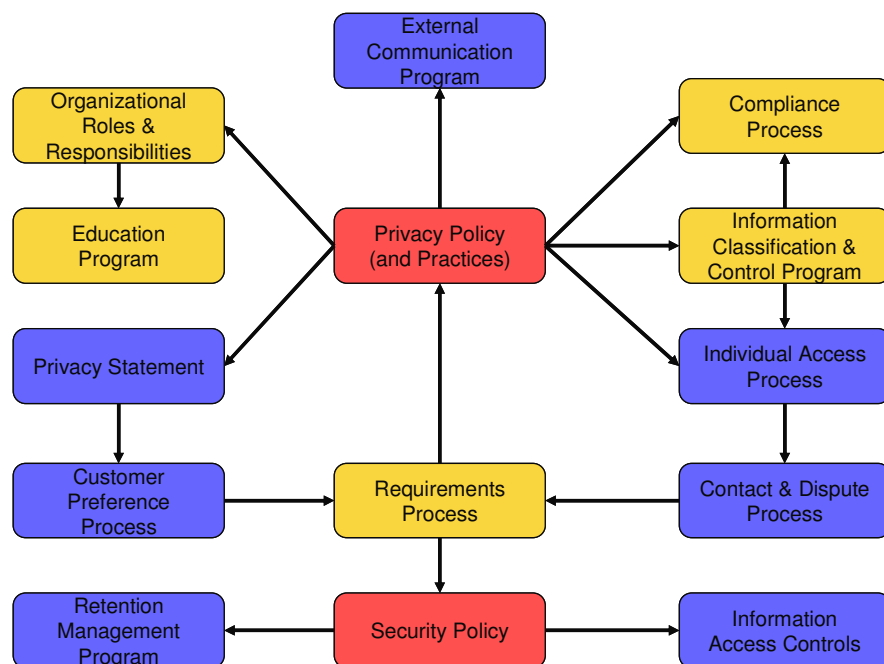
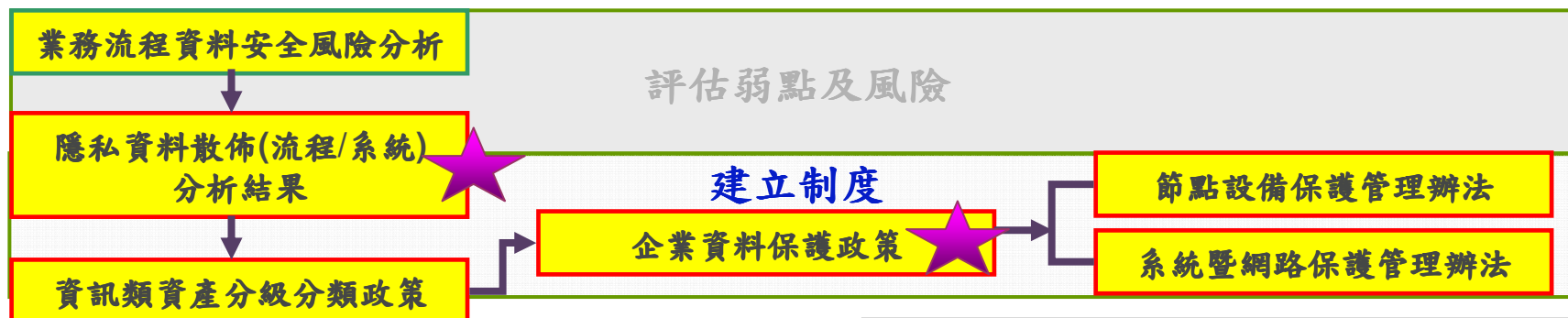


弱點及風險評估包含資料的取得、處理、儲存，網路、開發測試、應用程式、資料庫、儲存媒體等的弱點及風險檢測與評估



- 資料之生命週期防護架構差異分析
- 系統資料流風險分析
- 系統弱點及風險評估

企業資料保護政策以及隱私資料散佈分析結果是面貌掌控以及架構主體發展的重要指導方針



企業資料保護政策

- 企業之資料生命週期管理之最高方針及基準
- 資料生命週期管制要點

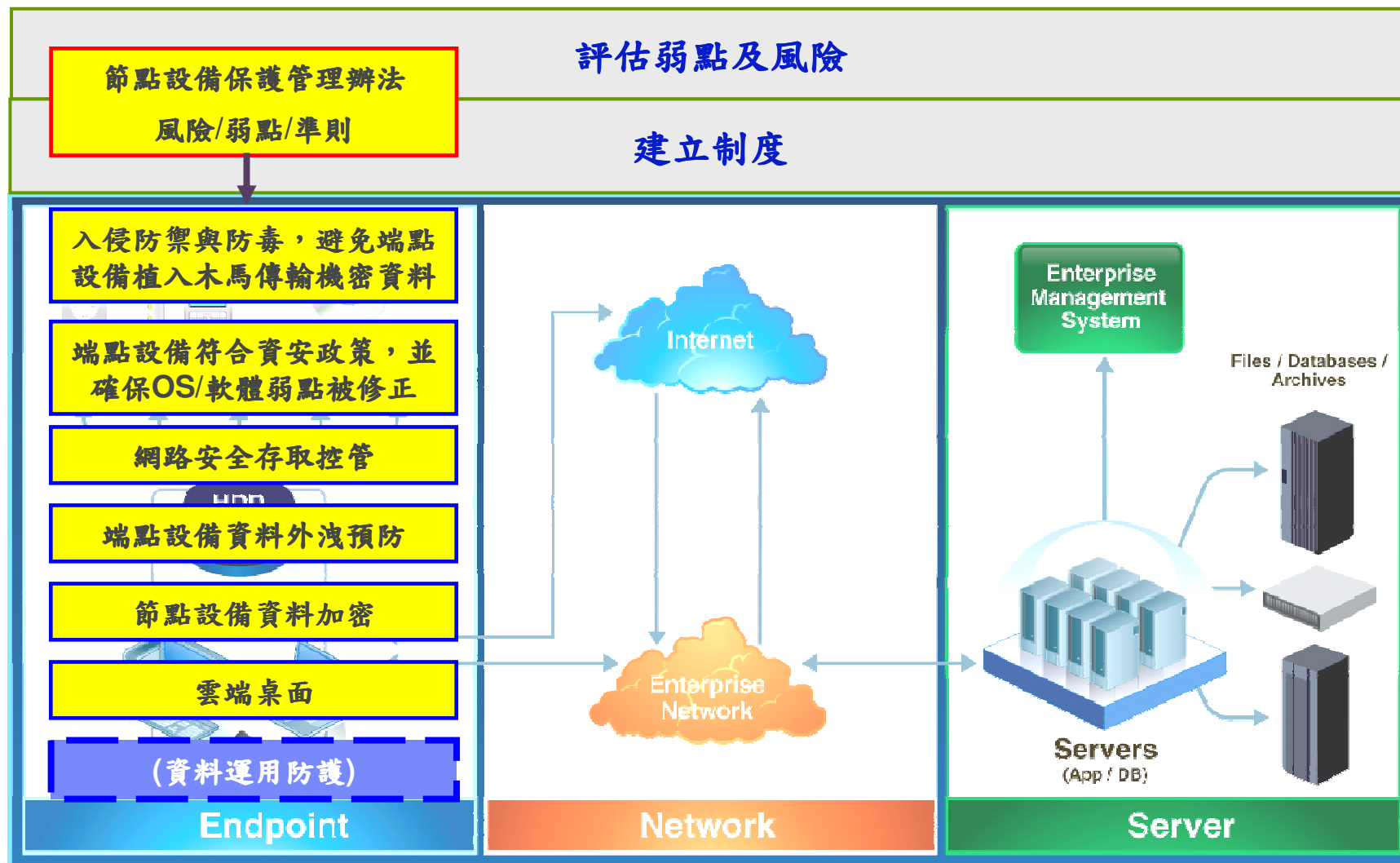
節點設備保護管理辦法

- 端點資料運用管制細則
- 節點設備設定及架構準則

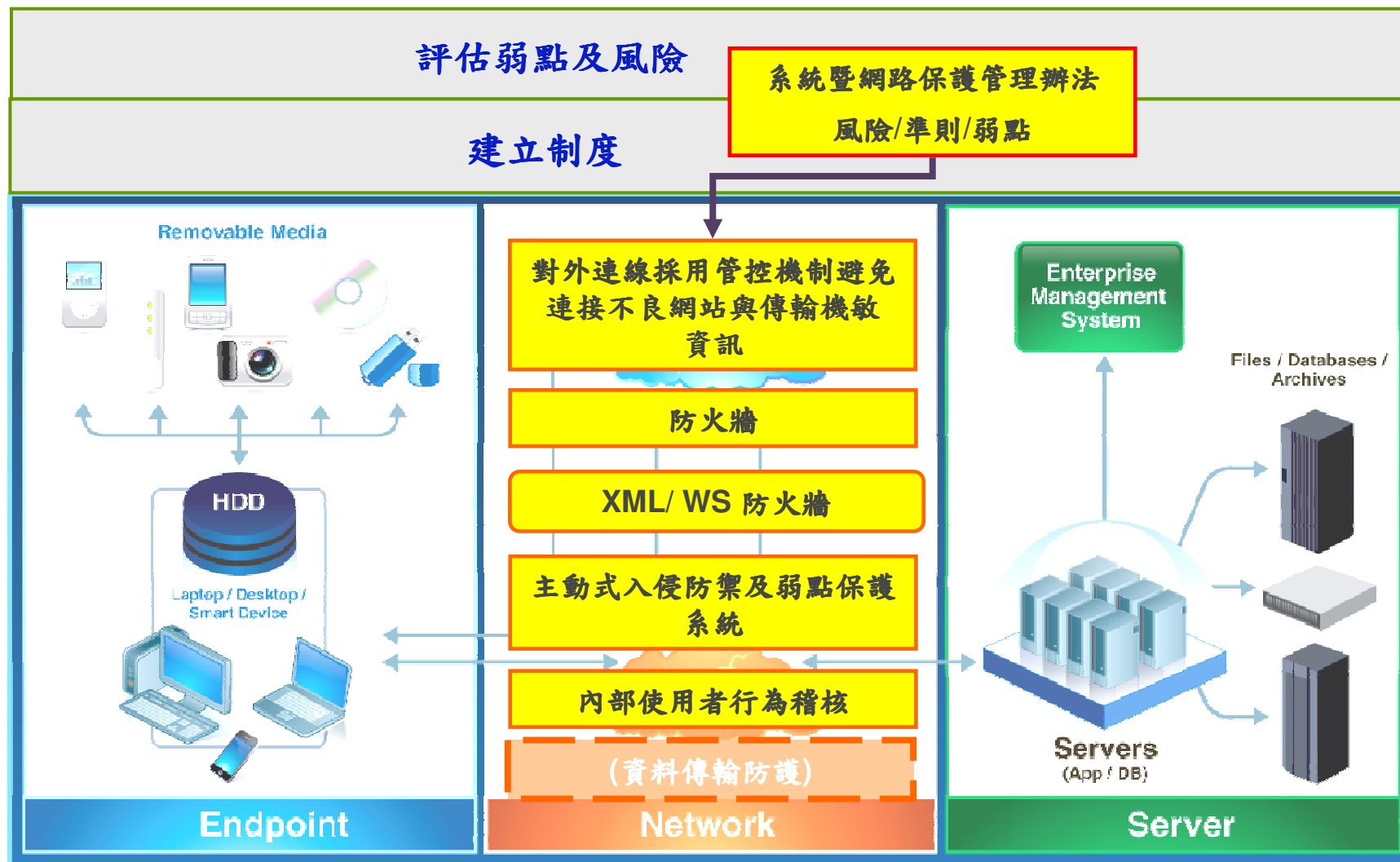
系統暨網路保護管理辦法

- 資料保存管制細則
- 系統設定及架構準則
- 身份辨認與授權規範
- 日誌收集及分析準則

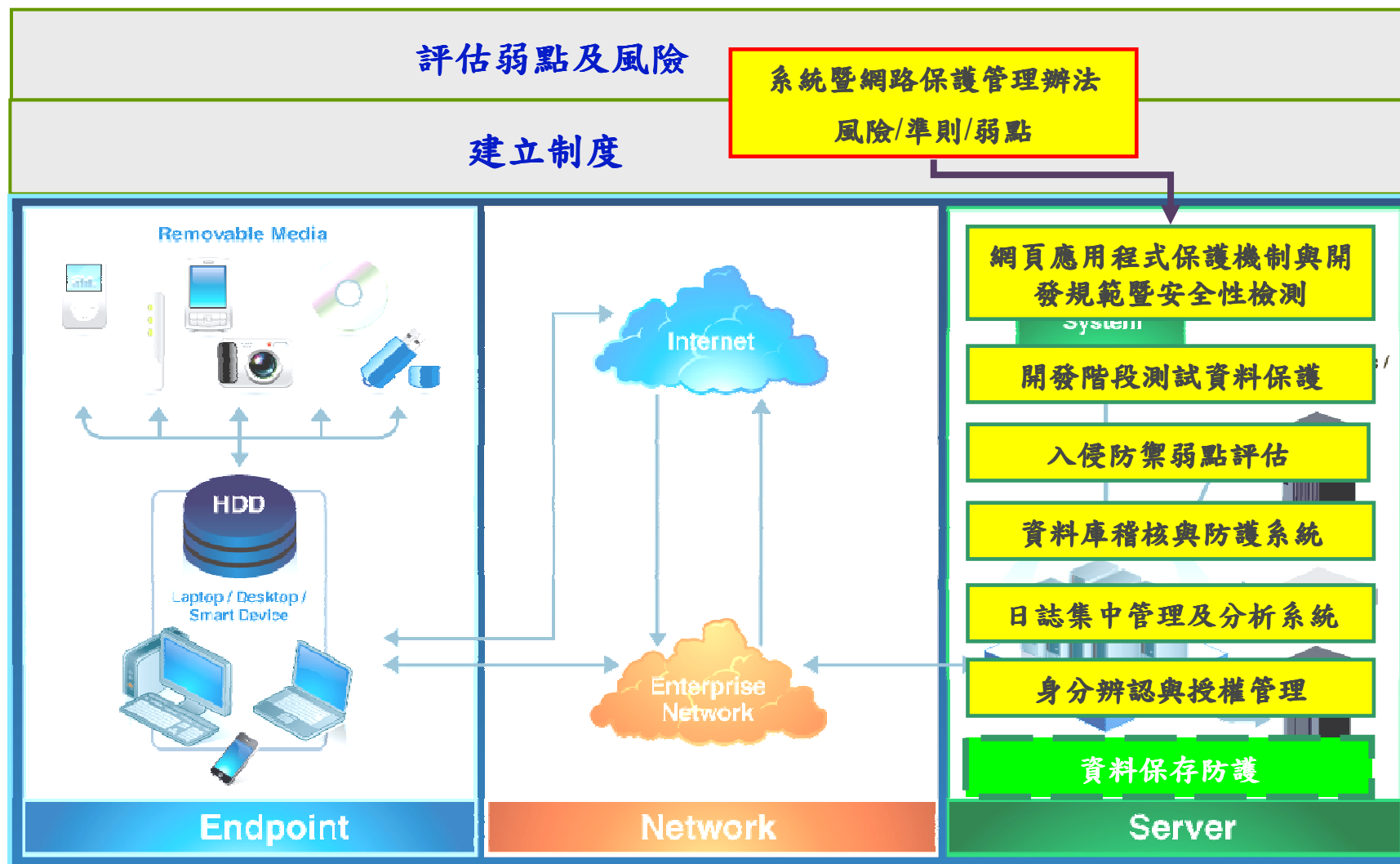
節點的資料安全中資料外洩預防、端點設備資料加密，甚至採用雲端桌面都是大部分企業可以加強的方案



網路資料安全中，Web防火牆是防護一般防火牆不檔的web通道，主動式入侵防禦是避免駭客入侵與隱碼攻擊竊取資料，而內部使用者行為稽核將電腦操作者的畫面輸出入資料錄起來更能達到舉證的效果

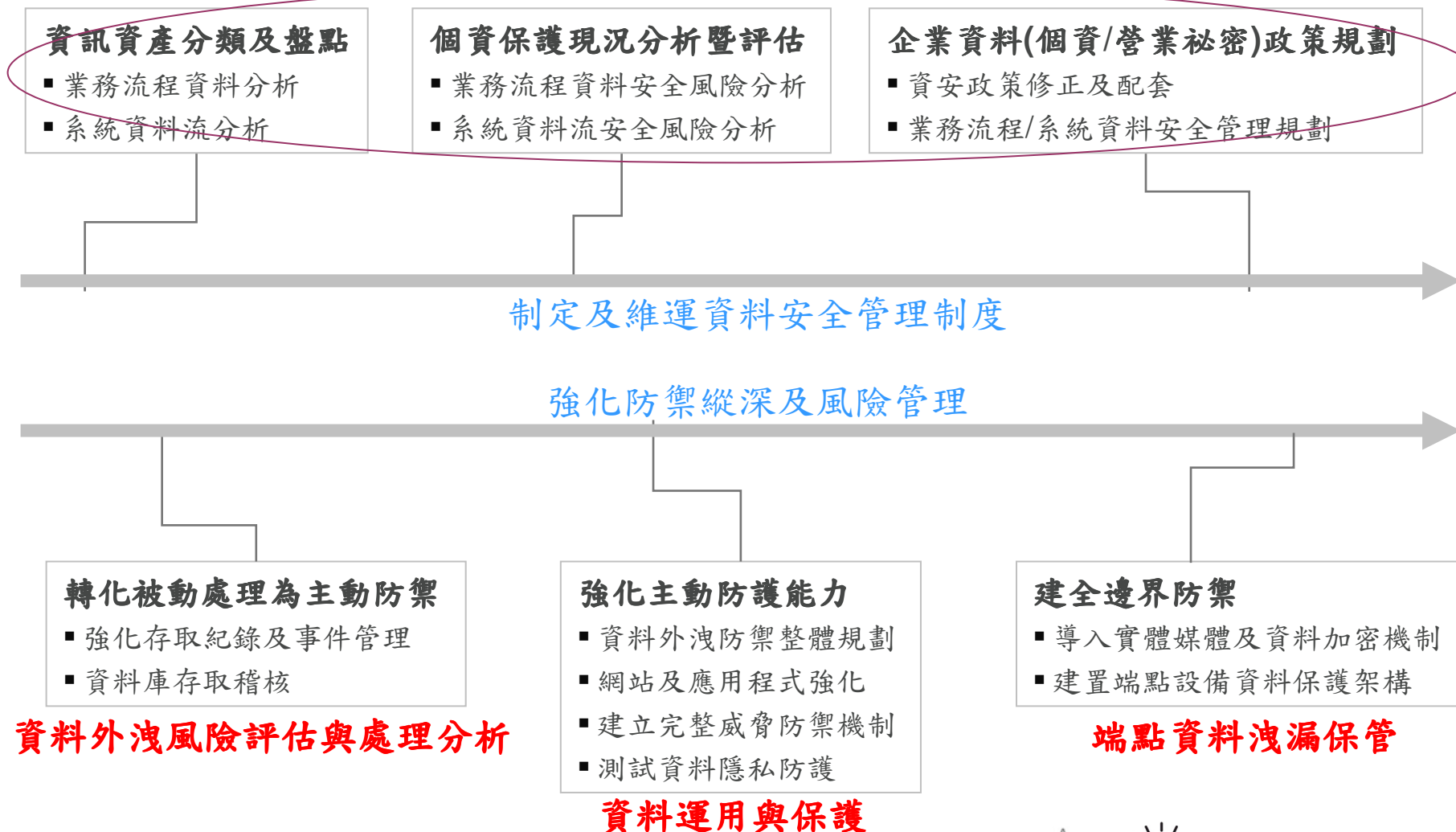


在伺服器端，資料庫稽核與防護能知道何人何時存取什麼資料，又不影響資料庫性能。而將散佈在各地的日誌集中管理及分析更是合規、舉證、稽核的重要功能。當然跨系統的身分辨認與授權是其中的基礎



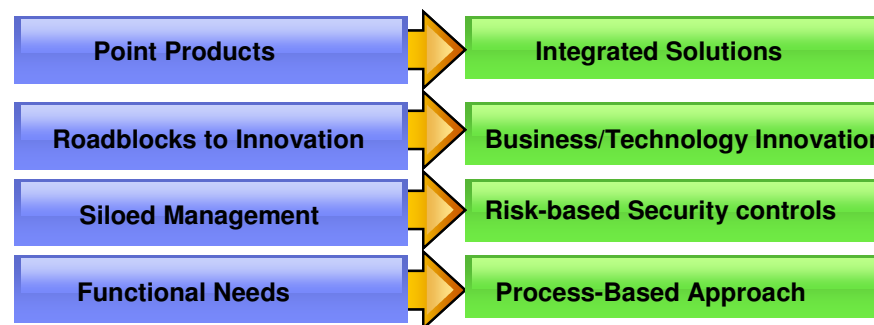
資料安全整體規劃藍圖建議

資安及隱私政策 / 業務及系統資料流程之安全管理



從「單點且缺乏業務處理流程整合」的產品導入方式，改為全方位資料處理的流程控管。從被動式的資安補強措施及方案，改為主動式的資料處理流程整合。

An alternative approach based on managing the IT security risk on business processes, not just the underlying IT infrastructure



執行策略及方向	預期效益
資安及隱私政策 / 業務及系統資料流程之安全管理	<ul style="list-style-type: none"> 瞭解隱私及系統資料散佈情形 掌控資料外洩風險及防護架構可能弱點所在 建立企業資料運用整體政策及準則
強化資料運用與保護架構	<ul style="list-style-type: none"> 導入資料保護及程式弱點檢測機制 模擬入侵測試，找出系統弱點 提昇主動式入侵防禦架構
健全節點資料存取及洩漏保管機制	<ul style="list-style-type: none"> 預防端點設備資料外洩 進行實體媒體(硬碟及磁帶)或資料加密 建立桌面資料防禦網
建立資料外洩風險評估與處理分析能力	<ul style="list-style-type: none"> 稽核用戶應用程式使用之異常行為 稽核資料庫查詢、異動及登入登出 日誌集中管理、異常事件分析及即時告警

Q & A

The technology is here.
 The people are ready.
 The time is now.



© Copyright IBM Corporation 2010

IBM Global Services
3-4F, No.7, Song Ren Road,
Taipei, Taiwan

Produced in Taiwan
All Rights Reserved

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Other company, product and service names may be trademarks or service marks of others.

IBM has the copyright to this material. The information in this document shall not be duplicated, distributed or disclosed to others in any form without IBM approval.

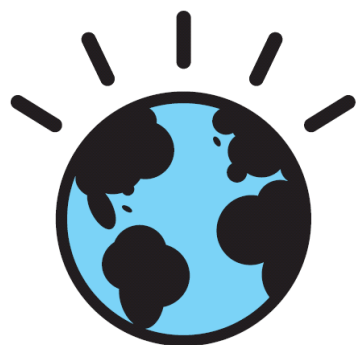


Benny MT KUO



附件

- IBM 各式解決方案細部簡介



IBM提供全方位的解決方案，選擇IBM是您明智的選擇

法規要求	IBM解決方案套餐	IBM 解決方案	產品對應
個資法	風險與弱點評估 制訂資安及 隱私政策	<ul style="list-style-type: none"> ■ 個資文件與資料分類分析與保護政策的訂定 ■ 制定個人資料保護政策並進行隱私資料流分析 	<ul style="list-style-type: none"> ■ GTS consultant ■ GTS consultant
應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏	資料運用與 保護	<ul style="list-style-type: none"> ■ 入侵防禦弱點評估諮詢與設計服務 ■ 開發測試階段資料保護弱點評估諮詢與設計服務 ■ 網頁應用程式保護機制與開發規範暨安全性檢測服務 ■ 主動式入侵防禦及弱點保護系統規劃與建置服務 <ul style="list-style-type: none"> ➢ XML/ WS 防火牆規劃與建置服務 	<ul style="list-style-type: none"> ■ GTS + Tivoli ISS Enterprise Scanner ■ GTS + IM Optim ■ GTS + Rational AppScan ■ GTS + Tivoli ISS IDS/IPS ■ GTS + WebSphere DataPower
	節點資料洩 漏保管	<ul style="list-style-type: none"> ■ 端點設備資料外洩預防規劃與建置服務 ■ 資料加密規劃與建置服務 ■ 磁帶端點設備機加密與保管解決方案 ■ 雲端桌面資料保護解決方案 	<ul style="list-style-type: none"> ■ GTS service (Digital Guardian) ■ GTS service ■ STG tape drive, library ■ GTS service (desk top cloud)
資料外洩損害賠償，非公務機構需證明「無故意或過失責任」，才能免責	資料外洩分 析與處理	<ul style="list-style-type: none"> ■ 內部使用者行為稽核規劃與建置服務 ■ 資料庫稽核與防護系統規劃與建置服務 ■ 日誌集中管理及分析系統規劃與建置服務 ■ 身分辨認與授權管理規劃與建置服務 	<ul style="list-style-type: none"> ■ GTS service (Intellinx) ■ GTS + IM Guardium ■ GTS + Tivoli SIEM ■ GTS + Tivoli Identity Mgmt, Access Mgmt

ISS：網路入侵防護解決方案

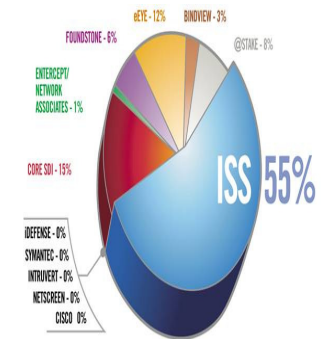
企業挑戰

當個資法通過後，如確保個資外洩問題？確認你的網路應用系統安全度？

- Web 網站使用了防火牆，所以很安全？
 - Web 網站提供對外服務，防火牆必須允許其通訊協定，但對於善意及惡意使用者並無法識別
- Web 網站使用IDS，所以很安全？
 - IDS 針對網路層之惡意行為進行過濾，對於以合法掩護非法之正常連結行為無法識別
- Web 網站使用了SSL 加密，所以很安全？
 - SSL 對於網站發送及接收之資訊都進行加密處理，但對於儲存於網站後端資料庫之機密資料並無法保障其機密性

誰最瞭解網際網路的風險？- IBM ISS X-Force 團隊

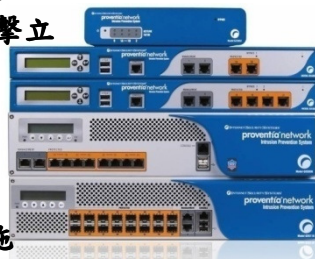
1. 長達14年的研發歷史
2. 專注於發現和分析安全風險，開發技術對策
3. 每半年發佈一次網路整體風險趨勢狀態報告
4. 每年發佈30 次以上的安全建議和警告
5. 每月找出200 多個新的攻擊手法
6. 維護超過 36,000 個漏洞的安全資料庫
7. 開發了 6000 多個檢查項用於檢測和發現攻擊手法
8. 發佈X-Force月度威脅觀察報告 (XFTIM)
9. 2008年，研究與發現7406個安全漏洞
10. CVE組織創始人之一，相容 CVE/CPE/ CVSS



高風險漏洞發現比例
Frost & Sullivan
2006, Internet

入侵防禦系統 Proventia® GX 價值主張

1. 全世界 IPS/IDS 市佔率 No.1 (包含台灣)
2. 有效偵測已知、未知攻擊行為，發現攻擊立即阻擋
3. 偵測 3,000+ 入侵攻擊
4. 支援「X-Force 虛擬補丁(Virtual Patch)」：使用者不必馬上更新系統的 Patch，即可在攻擊發生前完成防禦措施
5. 「虛擬 IPS」功能：依客戶環境同時支援超過「1,500」組以上監控防護政策
6. 高彈性佈署：線上模式、模擬模式、與監控模式。
7. 支援 HA 與 By Pass 模組，保障客戶「服務」不中斷



成功案例 References

1. 中鋼：入侵防護系統的部署有效阻擋了來源於外部的攻擊行為，也即時檢測出對於內部伺服器訪問的資料報文中是否存在可疑行為，並及時告警。
2. Grand Hyatt：簡化連鎖飯店的資安管理，及降低資安設備的投資，多合一的資安設備整合防火牆，入侵偵測系統，防毒，網站存取過濾等功能，有效防範日新月異的安全威脅。
3. 更多其他案例如：TSMC、UMC、Army、CHT、Sparq、CSIST、BOL、CA、SCB、Taishin Bank、TCB、DOH

型號	偵測埠	效能 / 保證頻寬	優惠售價 (未稅)
GX3002	2	10Mbps	NT\$ 288,000 (含第一年維護)
GX4004-V2	4	800Mbps	NT\$ 968,000 (含第一年維護)
GX5008-V2	8	1.5Gbps	NT\$1,968,000 (含第一年維護)

More information please contact Regina Chuang #9789

IBM Optim : 測試資料保護

Production System

- 提升生產力 **Improve Productivity**
- 提升系統效能 **Improve Systems Performance**
- 降低成本 **Reduce Costs**

Optim Data Archiving

- 提升服務水準(SLA)並降低風險
- 控制成本(硬體空間、軟體License、人力成本)
- 簡化 IT 基礎架構
- 實作符合成本效益的階層式儲存策略
- 滿足資訊控管需求
- 掌控快速增加的資料
- 透過資料生命週期管理(封存、儲存、存取、刪除)企業資料 (Data Life Cycle Management)
- 進行業務永續方案
- 增加企業應用程式的商業價值
- Garner report 調查現有客戶和潛在客戶，大家一致推崇和信賴 的產品

Non-Production System

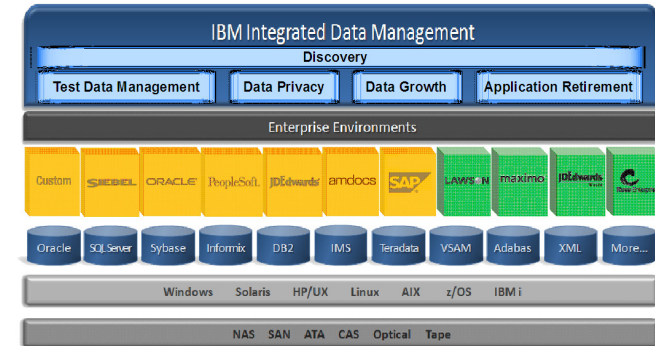
- 縮短測試時間 **Shorten Time-to-Market Schedule**
- 遮蔽機密資料 **Mask confidential data**
- 符合保密規範 **Comply with privacy policies**

Optim Data Privacy

- 遵循個資法，保護機密客戶資訊
- 避免罰款和處罰。避免負面宣傳（損害品牌形象，失去市場占有和收入損失）
- 符合特定行業和全球資料隱私的立法
- 保護公司（品牌資產/法律行動）
- 保護客戶（個人資料隱私/資料破壞）
- 使用各種已驗證過的資料遮蔽技術去遮蔽機密資料
- 使用有效的遮蔽數值來取代機密資料
- 保存遮蔽資料的完整性，使用於測試，培訓和系統開發的環境

Optim Test Data Management

- 減少線上作業系統停機時間與不可靠的應用性能
- 降低在正式作業環境中發現應用系統缺陷的成本
- 加速部署新的應用系統功能，及時支持客戶服務和業務計劃
- 在激烈競爭的商場，更快地提供產品和服務
- 建立符合實際、適當大小的測試資料庫，小到足以確保加快測試運行，但是又內含足以因應系統測試所需的完整資料
- 以快速便利的方式建立系統測試必需的臨界點資料，協助找出應用系統程式的缺點和不完善的邏輯
- 比較系統單元測試前，後資料的異動情況，新增、修改、刪除的差異結果，可以用不同顏色顯現於結果報表中，協助系統開發人員快速地驗證系統功能



AppScan : Web 應用程式零漏洞方案

企業挑戰

當個資法通過後，如何因應法規變化？要確保企業商譽與客戶關係，您準備好了嗎？

- 75%以上的駭客都針對網路應用系統攻擊，目前已經在運行的網站到底是不是安全的？
- 委外開發的Web應用系統，如何驗收確認其安全無虞？
- 網站應用系統愈搞愈大，功能愈來愈多，程式愈寫愈複雜，安全性怎麼兼顧？公司內部缺乏具備網站應用系統安全know-how的專業人員，就算你告訴我有漏洞，我們的人一時之間也不會改...除了委外處理別無他途了嗎？
- 網站才剛剛經過委外的資安專家檢測，目前沒有重大的漏洞，但駭客不斷研究新的攻擊手法，等到下次檢測還要好幾個月，這段時間不會有事嗎？

與競爭者的比較：市面上唯一整合黑箱與白箱的工具

1. HP WebInspect：無法提供符合國際認證標準的報表，在台灣無法提供即時的支援。
2. Fortify：其solution主要在於原始碼的靜態安全性分析檢測，支援檢測的開發語言類型眾多，但缺乏黑箱測試的解決方案，僅分析原始碼，會遺漏一些系統整合運行時才檢測得出的弱點，使用上也較侷限於開發人員。AppScan目前除黑箱測試的解決方案外，已有白箱測試解決方案，才是完整的安全性檢測管理方案。如果客戶都是委外開發暫大多數，其實不需要幫委外廠商購買白箱測試的軟體去測他們的程式碼，應該是購買黑箱測試的產品，確認程式沒有安全性的漏洞，才讓他們上線。
3. Dragonsoft, FoundStone等其他產品：OS/Network方面的弱點評估軟體，非網頁應用程式安全性檢測的產品。客戶容易混淆，誤以為網頁應用程式安全無虞了。

核心價值-產品功能

IBM Rational AppScan為Web應用程式安全性檢測軟體的先驅，市佔率世界第一。Gartner的研究預測至2010年，將有80%的企業會遇到應用程式安全問題。AppScan於整個軟體開發的生命週期中皆可應用，簡介如下：

- 是一套自動化弱點掃描工具，用來檢測Web應用系統的安全性，找出系統的資安漏洞，並一一提供詳盡的處理建議。
- 可簡化發現與修復Web應用系統安全性問題的工作，降低維護資訊安全的成本。
- 黑箱測試：模擬各種駭客攻擊的手法，以無害的方式去使用運行中的Web應用系統，判斷系統是否存在各種安全性問題，並按照問題輕重緩急順序，提供可立即處理問題的建議做法。
- 白箱測試：分析提供的原始碼，判斷系統是否存在各種安全性問題，指出有安全問題的原始碼位置，並按照問題的輕重緩急順序，提供可立即處理問題的建議做法。

成功案例 References

AppScan全世界超過2000個客戶。台灣應用成功客戶不勝枚舉，精選案例如下：(所有案例僅限IBM內部參考用，請勿隨意亂發)

1. 法務部: 資訊部QA人員，管理委外開發系統。
2. 工研院: 幫政府部門開發軟體，上線前交由電算中心測試後，再交給政府單位上線。
3. 北縣府: SEIM平台建置，確認上線的應用系統安全性。
4. 師範大學電算中心: AppScan建置前內部僅登記110個網站，透過Appscan掃描後發現漏登100個網站。
5. 尚有淡江大學電算中心等十多家大專院校電算中心已購買。

AppScan 急救包 單機版軟體 + 產品安裝與使用說明 -
超值優惠價：新台幣109萬

More information please contact Max Chen #9021

DataPower : Web Service 安全方案

企業挑戰

當企業邁向SOA整合環境，XML及Web Services將會扮演其中最重要技術腳色。然而不同資料間轉換，XML解析，Web Services執行效能或安全性及管理機制，是大多數IT經理和架構師邁向SOA即將面臨的一個主要挑戰！

- 正在考慮或使用SOA/ Web Service XML運用！
- 需要加密、解密或數位簽章與驗章安全的解決方案！
- 正面臨著將現有大型主機應用系統與SOA/ Web Service系統連接的難題
- 正面臨著XML訊息格式轉換的難題？

核心價值-產品功能

1. **Web 服務安全支援與存取控制:**支援SAML 及 WS-Security可控制內外部用戶端對 Web 服務應用程式的存取權並且能整合 LDAP以達到授權認證之功能。
2. **XML Denial of Service (XDoS) 保護:**能防止惡意使用者及型態異常資料破壞企業的應用程式伺服器或營運。如Single-message XDoS與Multi-message XDoS惡意攻擊
3. **XML 訊息加密與解密 Encryption/Decryption:**可執行各種基本的 XML加密、解密、數位簽章，即可將整個XML訊息或只將文件內某一個XML欄位加密/解密及簽章/驗證。
4. **XML/SOAP 防火牆功能**
支援過濾 XML 及 SOAP 資料流量，可防止惡意使用者及型態異常資料破壞企業的應用程式伺服器或營運。

“專”攻解決方案 Solutions

Data Power SOA 設備是業界第一個提供硬體解決方案的市場領導者

提供更安全SOA環境

-提供與外在系統連線時，系統間資料傳輸安全。如加密、解密或數位簽章與驗章

簡化SOA部署與快速整合

-利用革命性的技術在二進位文字及 XML 訊息格式之間轉換與繞送。協助實現安全的企業訊息匯流及系統整合。

加速 XML 處理程序

-可將常見的XML處理從伺服器或系統中卸載(offloading)下來進行加速，可加速大量的XML資料處理通常可有倍速效果

加強SOA治理 (Governance)與政策 (Policy)

-可擷取和連結 WSRR的服務，定期更新 Cache且針對服務擷取變動並執行時期原則與安全。

成功案例 References

客戶證言

「導入DataPower後，處理速率就明顯改善，現在處理過去兩、三倍的資料量都沒問題；其次，DataPower可協助在訂單資料進來及出去前先進行XML的格式驗證，一旦錯誤就直接擋信，此一驗證讓資料量大的公司可節省人力成本。」~宏碁集團資訊技術總處 資訊長 李文進

專案效益

1. 大幅增加系統整合與開發的生產力
2. 減少系統開發、測試時間、專案建置風險與導入期間並減少系統上市時機
3. 增加系統處理效率與系統處理資料量二~三倍
4. 增加擴充性和穩定性

WebSphere DataPower XI 50 定價 NT\$ 1,950,000 (未稅)

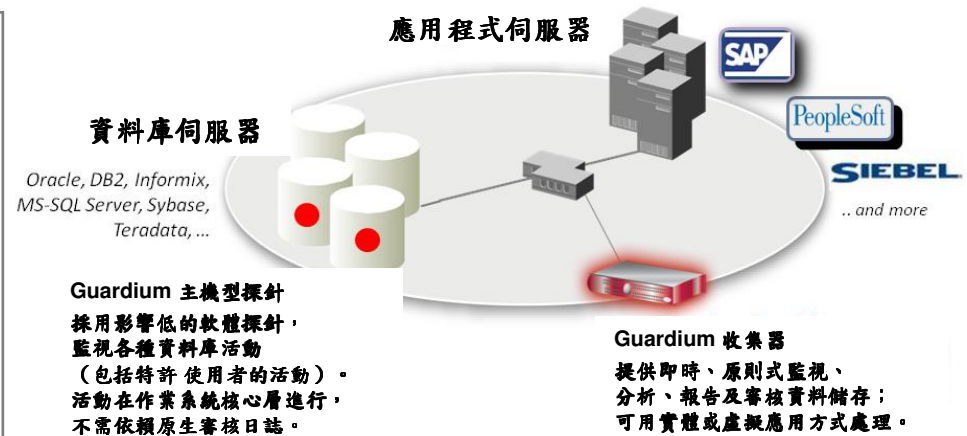
Guardium：即時資料庫監控、保護、及法規遵循

您知道嗎？

- 75% 的資訊外洩是由資料庫伺服器造成。
- Guardium 可支援 Oracle、SQL Server、DB2 UDB、DB2 for z/OS、DB2 for iSeries、Informix、Sybase、MySQL、Teradata。
- Guardium 的使用者包括全球前五大跨國銀行，全球前三大跨國零售商其中兩間，全球前六大保險公司其中四間，兩大全球最受歡迎飲料品牌和各大知名企業如 Dell、Accenture 和 McAfee.com。
- 法規遵循的最大重點在於 SOX（保護 ERP/財務系統），接下來是 PCI（智慧卡持有者資料）以及資料隱私。
- 對於財星五百大企業而言，Guardium 的投資報酬率為 239%，僅需 5.9 個月便能回收投資（Forrester 個案研究）
- Forrester 研究將 Guardium 譽為「本領域龍頭」，在「現有產品與服務」、「架構」及「產品策略」均為第一。
- 一般的企業交易額為 25 萬至 100 萬美元，而客戶若擴展到其他業務單位及應用，便會大幅增加附加交易。
- 一般服務：安全、遵規或風險目錄；DBA；應用程式架構；SOX 專案經理；基礎架構經理。
- Guardium 可專門著重監控資料庫層，輔助 IBM TCIM、TIM/TAM、及 ISS Proventia。
- Guardium 可支援異質的資料庫環境，輔助 IBM AME。

適用問題：您是否需要以下動作？

處理因資料庫控管不善而導致的審核問題。
為遵守沙賓法案 (SOX)，避免有人未獲授權而更改財務資料。
監控特許使用者，並實行職權分立。
避免資料外洩（例如 SQL 資料隱碼攻擊）。
找出資料庫的漏洞和遺漏的修補程式。
找出詐欺行為（使用 SAP、PeopleSoft、Oracle e-Business 等等）
減少遵規所需的人力和時間（各項法規如 SOX、PCI、NIST、FISMA、EU DPD、ISO 27002、資料隱私法等等）。
競爭對手：Oracle、Imperva、AppSec、Netezza/Tizor、Secerno、Sentrigo、Idera、Lumigent、NitroSecurity、Fortinet



輕鬆完成資料庫監控及法規遵循

產品主要特色

1. 非侵入性：Guardium 可持續即時監控所有資料庫行動，但不需改變資料庫或應用程式配置，也幾乎不會影響效能表現。
2. 異質性：支援各主要 DBMS 平台。
3. 降低作業成本：自動化處理各種法規遵循報告及監管程序（6 個月內回收成本）。
4. 擴充性：例如 Dell 已在全球 10 個資料中心超過 1000 台資料庫伺服器上部署 Guardium 以遵守 SOX、PCI 和 SAS70 等法規。Guardium 具備多層式架構、網路管理主控台、集中處理的跨 DBMS 稽核儲存庫，能夠達到集中處理的目標。
5. 職權分立：審核資料儲存於多個不同的實體或虛擬裝置中，內部人員或是駭客無法藉由篡改審核日誌資料來遮掩不法情事。這種作法不需仰賴原生的審核日誌（常駐於 DBMS 中），因此不需擔心被管理員輕易改動，便能確定職權分立。

政策及制度需透過持續不斷的教育訓練及宣導才能達到執行效益
除顧問服務之外，IBM亦可提供全方位教育訓練服務

IBM

Privacy - What you Need to Know

Welcome

Online Privacy Education for all IBMers

Welcome to 'Privacy - What you Need to Know'. This course explains IBM's approach to data privacy. Your awareness of IBM's data protection requirements will help you do your job. You will see that the proper handling of personal information goes to the heart of what it means to be a company built on Values, with trust and personal responsibility in all relationships.

Harriet Pearson
VP Regulatory Policy & Chief Privacy Officer
IBM Corporation

[Save my answers](#) [Restore my answers](#)