文⊙網擎資訊產品經理 簡經緯

備份電子郵件，保護企業智慧資產

想像一下這樣的狀況，企業正在研發的新產品，突然被競爭對手搶先一步申請相關專利，並準備推出相似的產品，追究原因是內部人員透過電子郵件將公司內部研發機密資料寄給潛在競爭對手。但當企業需要用電子郵件舉證時，一方面不知道茫茫大海的電子郵件要如何找起，另一方面郵件可能早已不存在郵件伺服器中

電子郵件洩密的事件，在你我的現實世界中每天都在上演，公司許多寶貴的無形資產透過電子郵件不當的外流，造成企業重大的損失。根據日本調查報告顯示，企業資訊洩密案件有高達 70% 是由公司內部洩漏所造成，若能及早做好郵件防護機制就能有效降低機密外洩的可能性。

從另一個角度來看，根據 Enterprise Strategy Group調查：電子郵件已經成為商務溝通最常使用的工具，企業員工每年平均會收到25000封的電子郵件，因此企業的智慧資產有75% 都存在電子郵件媒介中，這麼珍貴的無形資產如果妥善運用，可以為企業帶來更多潛在的商機。

可惜的是，目前企業對於資料庫等資訊系統都有設定相關資訊安全或備份機制，但是對於電子郵件這道缺口，卻鮮少有IT單位規畫進行郵件資安防護與備份管理。

遵循郵件備份法規是責任，更是義務

美國在經過安隆（Enron）、世界通訊（WorldCom）等一連串上市公司財務報表不實及公司管理失當的醜聞後，投資大眾頓時喪失對證券市場之信心，為重拾投資大眾之信心，美國國會迅速通過沙賓法案（Sarbanes-Oxley Act），要求上市公司與會計師必須將所有的記錄保存至少5年，與會計相關的文件則必須保存至少7年的時間，若不符合法規規定企業必須罰款，嚴重違反法規的企業CIO還必須入獄服刑，舉例來說2005年2月JPMorgan Chase & Co就因為無法於期限內繳交美國SEC要求的內部證券研究報告，而被罰以200多萬美金。

除了美國 2002 年制訂「沙賓法案」（Sarbanes-Oxley Act，SOX）、日本亦於2005年4月通過「個人情報保護法」與預計在 2008 年實施的「日本版沙賓法案」外，臺灣目前金管會也對相關金融機構有類似規範，將針對金融業所實施「新巴塞爾資本協定」（Basel II），其中規範到企業資訊備存與電子舉證（Electronic Discovery）機制的建置，讓郵件不再僅止於病毒及垃圾信的防護，企業也需要考慮郵件的備份、備援、稽核、歸檔及搜尋等問題。

處於一個國際化社會，臺灣與歐美、日本貿易往來頻繁，在全球供應鏈整合趨勢下，臺灣企業同樣面

美日兩國相關的法案規定

影響產業	相關法規	法規概述
全部產業	沙賓法案（Sarbanes- Oxley Act of 2002）	企業有責任將所有的電子檔案以及電子郵件紀錄，備份保存至少 5 年。
會計與財務相關機構	沙賓法案（Sarbanes- Oxley Act of 2002）	為了讓企業營運及財務資訊更加透明化，財務以及會計相關機構與企業，必須將審計相關文件保留 5 年以上，查核報告資料則至少需保存 7 年。
	SEC 17 CFR Part 210	根據美國證券交易委員會規定，與財務報告審核相關的工作資料以及檔案都需保存 7 年以上。
醫療產業	HIPAA（Health Insurance Portability and Accountability Act of 1996）	無論是電子郵件或檔案，包括與公司往來合約、與醫療政策及流程相關的文件、與病人溝通的紀錄表格或是消費者抱怨等紀錄，都需保存至少 6 年。此外，所有與病人相關文件最少需保留至病人過世後 2 年。
全部產業	個人情報保護法	規定企業或團體組織有義務保護個人資料防止洩漏，需保存資料並確保可有效取得。違反將處以 6 個月以下，及 30 萬日幣罰金。
金融相關產業	日本版沙賓法草案	根據 302 條，企業有義務公開有價證券報告和財物報表並宣示正確性。同時，根據 906 條，無論刻意與否遺失財務報表而造成重大損失，將處以刑事罰則，若刻意遺失，則最高可處 20 年懲役、罰金 500 萬美元。

臨到需配合建置郵件備份相關法規遵循的課題。目前各國對於郵件備份的政策和法規不盡相同，但基本上有三個共同的原則要求：

郵件資料的完整歸檔

* 資料保存必須完整。
* 在法規限制年限間，資料不能刪除。
* 保證資料在保留年限內，絕對可用。
* 要可以快速查詢到保存的資料，保留的資料要標準化，未來若更換新技術，資料還是可以存取。

隱私權與安全性

* 保留的資料不可以被非法使用。
* 應要有權限規定。
* 隱私權的規定。

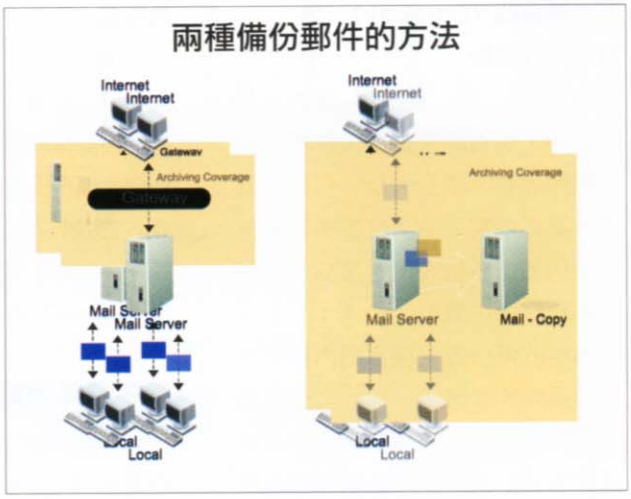
追蹤存取記錄

* 資料的新增、修改、刪除記錄都要保留下來。
* 存取記錄不能被任意刪除。

善用企業智慧資產

據Forrest Research的調查統計資料顯示，企業的無形資產中有20%左右的資訊，有效地儲存在各種類型的結構化資料庫中；但是還有80%非結構化或半結構化資訊（文件檔案、電子郵件、多媒體等），如分散於組織間與個人電腦中，其中尤其以電子郵件所佔的比重最大，換言之，電子郵件其實是儲存企業中最珍貴資訊的知識寶庫。

企業可以針對電子郵件知識庫挖掘出許多有用的資訊，提供其他員工再利用，進而引發更多隱性知識。許多企業推動知識管理成效不彰，主要原因是員工再重新適應另一套新的系統會產生抗拒感，同時企業要求個人上傳工作檔案到知識庫中，會讓員工覺得增加工作負擔加重。但是如果使用電子郵件作為知識管理平臺，因為員工平日就習慣使用這個溝通工具，可以加速企業知識管理的導入。



而在電子郵件知識管理過程中，亦要注意權限管理與隱私權的問題。舉例來說，總經理與人事部門之間談論員工薪資的郵件，就不適合出現在電子郵件知識庫中。哪一類電子郵件不可以被搜尋到？哪一類電子郵件可以被搜尋到但點選開啟檔案時需要身份認證？這些都需要事前規畫，才不會造成企業機密外洩。

電子郵件系統備援與資料備份

在整個電子備份機制中最重要的兩個因素：如何備份？與如何快速找到備份的信件？以電子郵件的備份來說，要注意到電子郵件系統備援與電子郵件資料備份的差異，這兩者的目的及方式均不相同，但對於企業來說都同等重要。

電子郵件系統備援

在郵件伺服器遠端架設一臺與郵件伺服器相符的備援伺服器，透過網路定時更新備援伺服器的資料，所以當郵件伺服器當機時，另外一臺備援的伺服器可以馬上取代原有伺服器的工作，可讓系統的停機時間降至最低，並可確保資料的完整性，讓企業郵件伺服器服務能於最短時間內恢復正常工作。

通常透過備援工具，如rsync，以增量備份 （incremental）定期將整個郵件伺服器系統資料複製到另外一臺備援機器上。若備份時間點設定的越頻繁，當災難發生，備援的機器會越接近原來機器的狀態。

電子郵件資料備份

將所有進出郵件伺服器的郵件，甚至連被刪除的信件都完全備份下來，不是把整批信件備份下來，而是一封一封信件備份到備份伺服器中。主要區分兩種方式：

第一種：

郵件備援與備份比較表

	電子郵件系統備援	電子郵件資料備份	
目的	24小時永不停止郵件服務	滴水不漏地備份所有郵件	
方式	透過備援工具，如rsync，以增量備份 （incremental）定期將整個郵件伺服器系統資料複製到另外一臺備援機器上。	利用閘道器方式	利用郵件複製方式

利用閘道器（Gateway）方式進行備份

在電子郵件伺服器前端放置一臺閘道器，所有需要進出信件都必須經過閘道器，並且備份一份信件到資料庫或檔案庫中。缺點是若郵件閘道伺服器當機時，會造成整個郵件系統停擺，風險會較高；另外，閘道器的備份方式會忽略內部寄送內部郵件的備份。

市面上大部分搭配的閘道器通常還需整合防毒、防垃圾信等機制，通常會給人感覺可以一次購足所有的解決方案，但要注意若再加上備份電子郵件功能，往往會造成效能過慢，影響到後端郵件伺服器的運作，這也是選購電子郵件備份方案時需要考量的部分。

第二種：

利用郵件複製（Mail-Copy）的方式

在電子郵件旁邊建置一臺電子郵件備份伺服器，利用側錄的方式將所有進出郵件伺服器的信件複製一份存到郵件備份伺服器中，優點是利用側錄方式完全不影響郵件伺服器的處理效能，亦可確保滴水不漏備份到所有進出與內部互傳的信件。

電子郵件搜尋與調閱

處理相關證據時，美國法院規定企業必須在24到48小時內，提出所需要的證據，若系統沒有搜尋機制，如同大海撈針勢必無法在時間內完成法規規定的要求，因此一套有效的搜尋機制對於電子郵件備份來說是非常重要的。郵件搜尋主要區分兩種實作方法，即索引庫檢索及資料庫檢索：

索引庫檢索

透過搜尋引擎建立所有信件的索引庫，加速搜尋，當使用者要搜尋備份的信件，先搜尋索引庫然後導引到原始的信件。要注意的是目前大部分的信件會夾帶許多附件檔案，搜尋引擎必須能支援搜尋到附件中的文字內容。

資料庫檢索

利用資料庫SQL語法檢索郵件的Metadata欄位資料，當進行大量資料檢索及排序時效能不佳，且無法搜尋到信件附檔中的內容。

政策是導入郵件備份關鍵

企業準備電子郵件備份前，先想一想企業的電子郵件備份政策（Backup Policy），備份的目的，是為了企業知識管理或者只是要符合法規規定？哪些人的信件需要備份？希望保留多久時間，是不是時間到就可以刪除或移到其他儲存媒介？備份資料如何保護與保存？隱私權與權限的問題，是否需要加密與需要哪些Log資訊？這些因素都會影響到企業電子郵件備份規畫方向，只有在事前完整的評估，才能打造一個符合貴公司的電子郵件備份方案。

作者簡歷：

網擎資訊產品經理 簡經緯

網擎資訊行銷業務部資深產品經理，美國羅倫斯科技大學電腦科學碩士，曾任職於碩網資訊產品經理及技術顧問，主導智慧資本管理平臺、文管系統規畫與開發，並通過CMMI Level 3 認證。專長於企業文件管理、知識管理、智財管理、郵件安全整合方案等。

專家建議

全面檢視郵件資訊安全防護策略

近年來，病毒信與垃圾信防制的議題搭著資訊安全的熱潮，多數企業均意識到電子郵件內容管理的重要性。為了避免病毒信肆虐的危害與垃圾信充斥的混亂，企業紛紛投入心力對抗病毒信與垃圾信，務求還給員工一個清爽乾淨的收信匣。但我們不禁要問，郵件資安不僅只有垃圾信與病毒信，這樣就能確保郵件系統的順暢與安全嗎？

整體規畫郵件系統的資安策略

企業架設電子郵件系統不外乎是希望建立一個穩定、快速、安全的訊息溝通環境，除了解決郵件內容安全面向的病毒信與垃圾信問題外，在系統安全、郵件稽核、系統備援、郵件備份與使用行為分析上，都應該納入全盤考量，以宏觀的角度整體規畫郵件系統的資訊安全策略。例如，短時間大量不正常的SMTP連線可能會造成郵件系統癱瘓，如果可以在第一時間將這類的垃圾信或字典攻擊的連線阻絕在系統外，可以大幅節省頻寬與硬體資源。此外，為了確保郵件系統持續正常運作與迅速災後復原，部署系統備援與郵件備份機制亦是刻不容緩的課題。

強化郵件資安體系已是大勢所趨

隨著企業倚賴日深，電子郵件系統已躍身成為企業內相當重要的資訊系統之一，更是信息溝通以及商務往來的重要命脈。因此，企業應避免針對單點問題導入個別的產品，建議應透過整體規畫來強化企業郵件資訊安全機制，因應相繼而來的各種挑戰。

－網擎資訊專案經理周宇軒