Openfind Software Engineered for Growth

郵件過濾與稽核管理，為企業治理增添效益

Openfind 產品經理 張世鋒

過去資訊安全的討論範疇裡，從各種外來的弱點攻擊到病毒防禦等問題，不斷被討論，但是企業的訊息安全（Message Security）議題在所有資安問題中所佔的比例不到 3 成，而就在近幾年來垃圾郵件問題嚴重化之後，加上各種翻新的攻擊手法與企業內部機密資料外洩等問題，企業不得不面對與重視訊息環境所帶來各類的災害與資安風險。而從企業使用率與資料傳輸的角度來觀察，莫過於電子郵件的應用。

企業訊息安全的發展

當今電子郵件的應用已經產生重大轉變，從單純的文字訊息傳輸工具轉變為企業與個人高度依賴的主要溝通平台，未來郵件相關法規通過後，郵件更可能成為正式商務文件，成為具有法律效力的電子文件。因此，企業在享受電子郵件便利的同時，應思考相對應的企業責任與一直被輕忽的隱藏風險。除一般軟硬體設備、網路環境、郵件管理政策等因素外，郵件系統能否妥善管理與整合大量資訊，避免工作時程延遲；或者郵件訊息處理效能不足，無法及時傳遞訊息。除了效能問題，另外還必須納入郵件安全防護與備份管理的機制，整體規劃企業郵件訊息安全環境，確保溝通競爭力並妥善管理使用行為。

安全防護與備份管理

面對網路上任何不安全的因素，如病毒、攻擊、不當內容、廣告郵件等，系統是否具備足夠的防護能力？大多數的企業雖已建置病毒與廣告信過濾系統，但仍欠缺安全防護的整體規劃。例如因郵件系統不穩定、大量垃圾信與攻擊信造成營運停擺。而企業若沒有進行郵件備份，當郵件訊息均由員工下載至個人電腦時，則備份週期或嚴謹程度是否符合企業需求？或者企業雖規劃郵件備份，但如何從大量歷史信件資料找到所要的資訊？最後就是龐大的管理成本問題，面對每年以 40% 成長率增加的企業郵件，如何保存這些流動的訊息（包含信件中雙方業務往來的資訊、流程的記錄）加以有效管理與完整備份，來符合法規遵循與郵件政策皆是企業必需規劃的課題。

企業該如何看待企業治理

企業治理（Corporate Governance）就目的而言是「**加強公司整體效率，塑造健康的企業治理文化，提升企業競爭力**」。而在美、日紛紛制定郵件相關法規之下，以美國沙賓法案（Sarbanes-Oxley）為例，從今年開始適用於在美國掛牌的外國企業，如台積電、聯電、友達等跨國大型製造商，則因與美國企業有商業往來，

都必須開始注意是否符合相關規範，做好企業治理的工作。當電子郵件成為法律上的有效文件，這顯示要做好企業治理，防止企業商譽受損，急需思考如何做好郵件治理的工作。

前過濾與後稽核，打造完整郵件治理

目前各企業的郵件安全的作法，已由被動式的防禦轉為主動式的防護，當今企業郵件安全不僅止於阻擋垃圾郵件與各種病毒威脅，更需配合組織內現行群組架構，進行郵件內對外過濾、外對內防護機制。前端建構完善的防護機制後，接下來就是規劃後方稽核管理做法，稽核管理是以降低內部資安風險為目的，因此符合企業使用的郵件備份系統要提供完整保存郵件的能力，同時具備搜尋、調閱、權限控管等功能，並可落實資訊生命週期管理（ILM）的規劃，與彈性的儲存硬體整合能力。

郵件寄送前過濾	**郵件備份與後稽核**
前過濾重點：**預防** 優點： ● 可疑信件直接隔離 ● 採事前預防，避免損害 ● 彈性的過濾規則管理 ● 落實郵件政策，有效治理 問題： ● 垃圾郵件範本精確度？ ● 是否影響正常收發信件？ ● 增加主管工作負擔的可能？	後稽核重點：**調閱** 優點： ● 完整保存郵件資料 ● 不影響正常收發信 ● 信件留存，保留證據 ● 降低郵件遺失風險 問題： ● 採事後確認，損害恐已造成。 ● 軟硬體災難之復原與控管。 ● 儲存設備規劃問題。

面對未妥善規劃的郵件訊息環境所帶來的高度資安風險，企業應先釐清應用需求並制定郵件政策，並清楚的與企業員工進行溝通取得共識，再進一步落實郵件治理工作，以杜絕不當的使用行為與衍生風險。透過前方郵件過濾與後方稽核管理，可以保障企業訊息安全，提高企業生產力與溝通競爭力，落實企業治理以及建構安全可靠且完整的郵件訊息溝通環境。