當組織發生事故時，災害復原能力是持續營運不可或缺的重要部分。

營運持續計畫之災害復原實作

◎紀佳妮

一、前言

營運持續管理（Business Continuity Management, BCM）是一個全面性的管理過程，對於一個組織而言，最終目標不外乎是實現組織的永續經營。在組織規劃完善的營運持續計畫（Business Continuity Planning, BCP）中，災害復原計畫（Disaster Response Planning, DRP）是組織營運之重要環節。當組織發生事故時，災害復原能力是組織持續營運不可或缺的重要部分。災害復原的目的是為了在發生天災、人為疏失或惡意破壞造成資訊系統損害時，能以災害復原機制快速回復至組織正常或可接受的營運水準，以確保組織的永續經營。

災害復原計畫包含資源重置、採用備援措施、緊急應變處理與營運復原，藉以縮短災害發生對營業中斷的影響時間或加速復原速度。

二、災害復原計畫實作階段

(一) 診斷與分析

針對組織的資訊科技應用現況、資訊科技應用需求、相關資訊科技資源項目，以及事故發生後，可能導致的資訊系統失效或資訊服務中斷等狀況來進行分析與評估，建議資訊部門應與相關部門共同攜手合作。一般而言，組織應考量哪些資訊服務與維持組織營運持續能力有密切的相關，分析並找出組織的關鍵資訊業務最大可容忍的中斷時間、制定關鍵業務流程之復原時間目標（Recovery Time Objective, RTO）與復原時點目標（Recovery Point Objective, RPO）及評估關鍵業務流程所需之回復資源項目。

(二) 備援方案與架構

基於診斷與分析所得出來之「關鍵業務」，這裡我們以資訊系統與資訊服務業務，規劃出相對應的備援方案及其應用架構於災害復原計畫。災害復原計畫應面面俱到地闡明整個復原過程。以下幾點應納入計畫擬訂的要點，包括：

1. 什麼樣的事件可能會引起災害？
2. 什麼人有資格宣布組織已經進入災害狀態，並啟動災害復原計畫？
3. 啟動災害復原計畫後，準備備援地點的所需步驟？
4. 所有實施計畫的關鍵人物所扮演的角色與承擔的責任為何？
5. 復原過程所需的硬體與軟體？
6. 從備援地點轉移回原營運場所（或移到新地點）的步驟？

因此災害復原計畫撰寫內容至少應包括：

1. 災害復原計畫的目的：說明災害復原計畫制定的目的與災害的定義。
2. 災害復原計畫的範圍：說明災害復原計畫所涵蓋的資訊業務項目。
3. 計畫發展程序與流程：說明計畫制定的流程，並列出制定過程中需參與之部門／人員，以及所負責執行之工作項目。
4. 災害復原計畫管理機制：說明災害復原計畫的管理方式，建議可成立相關計畫管理組織（例如委員會），並進一步說明管理組織的人員組成、工作執掌，以及管理機制的運作方式。

制定災害復原組織時，建議組織架構以架構圖呈現。委員會可設立召集人或主席，而各小組可依照資訊業務內容與複雜度再細分為不同的工作分組，選擇組織內適當的成員加入各小組。例如機房維運人員、資料庫管理人員、系統維護人員，均可同時加入應變處理小組處理與回復作業小組。

5. 災害通報程序：建議用流程圖來說明災害通報程序，並且列出相關通報權責單位，以及根據災害所造成之損失程度來設計通報升級條件。
6. 受災後應回復之服務水準：列出關鍵業務之組織可接受的最低服務水準，且經管理階層同意。
7. 回復所需資源：考量回復關鍵資訊業務所需的資源包括：
   (1)回復所需之場所：如資訊系統運作場所、人員操作場所及人員辦公場所。若單位考量採用異地備援場所，其評估重點包含：原營運場所發生重大災害時，備援場所是否也受到災害影響而有所毀損；可存取的時間是否符合需求；環境是否可支援所需設備，包括電力與網路管理控制等。
   (2)回復所需之硬體，如伺服主機、網路設備等。
   (3)回復所需之軟體，如作業系統、資訊應用系統、資料庫管理系統等。
   (4)回復所需之通信網路，如電話通訊服務、網路通訊服務等。
   (5)回復所需之其他資源，如辦公室用品、傳真機、影印機等。
   (6)針對系統備援機制方面，組織可依據對於回復時間目標的要求、回復時點目標之規劃、相關投入之成本、現有資源狀況等，以評估最適合的備援機制。有關系統的備援方式與比較說明，詳見表１。

表1　系統備援方式

測試方法	說明	回復速度	投入成本
熱備援場所（Hot Site）	擁有所需完整、設定好的、軟硬體和各項必要的工作環境（如網路），並隨時待命。	快	高
暖備援場所（Warm Site）	具備電源、空調、通信和高架地板等基礎設施，及某部分執行環境（某些硬體、周邊裝置），但沒有完整的設備或軟體安裝。	中	中
冷備援場所（Cold Site）	只提供緊急事故時可以繼續運作的建築空間，擁有電源、空調等基礎建設，但沒有任何電腦硬體。	慢	低

資料來源：自行整理

8. 災害復原回復程序：可針對不同之災害復原用資源項目進行回復規劃。例如可針對資訊應用系統、資訊機房、資料庫與通訊網路服務訂定相關回復作業流程與步驟，而這些作業流程與步驟建議以標準作業流程（SOP）的方式呈現。
9. 災害復原備份程序：考量備援環境之後，資料庫的完整性與還原效能同樣重要。資料備份時應注意備份排程之完整與完善，並且進行備份保存與存放位置之規劃，留下完整的紀錄保存工作表，包含使用單位、種類、媒體形式、容量等相關資訊。備份媒體存放於何處，對於備份回復所需之時間與努力有很大的影響。但災難（例如火災）發生時，資料備份若在上線環境可能也會損害，所以許多組織將備份資料異地存放。關於備份類型大致可分成下列幾種，單位可以評估需求，訂定備份策略。常見之資料備份類型，詳見表２。

表2　常見資料備份類型

備份類型	說明	備份時間	回復時間
完整備份	將要備份的檔案完整地保存一份在備份儲存媒體中（把全部檔案進行備份，並把已備份的檔案標示為已備份）	長	快
差異備份	備份上次完整備份後，內容有變更或新增的檔案（只備份經修改的檔案，或新建立卻沒有標示為已備份的檔案，但不會把已備份的檔案標示為已備份）	中	中
增量備份	備份上次完整備份或增量備份後，內容有變更或新增的檔案（只備份經修改的檔案，或新建立但沒有標示為已備份的檔案，並把備份後的檔案標示為已備份）	短	慢

資料來源：自行整理

8. 災害場所復原作業：內容包括災害場所清理方式、災害場所復原規劃、災害場所回復作業及人員回歸原營運場所工作之相關作業方式。
9. 附件：列出緊急聯絡清單，內容應具有：
(1)對外連絡清單應包含下列單位：當地警察局、消防隊、維護或供應廠商、重要媒體及上級主管機關等。
(2)對內聯絡清單應包含災害復原計畫相關人員與各部門重要人員。

(三) 導入管理

實施已規劃完成之災害復原計畫、相關備援方案及應用架構，並建立適當的計畫管理機制，以確保計畫導入建置過程的有效性。為避免災害復原計畫版本誤用，災害復原計畫應文件化，並設定文件控管機制，包括災害啟動、判斷及動員之程序文件、重要紀錄恢復文件、 IT系統回復程序文件、網路與通訊文件、應用系統與資料同步檢查表文件、手動操作程序文件等等。災害復原計畫應視業務、組織及人員的調整需求而進行維護更新。每年應至少一次評估災害復原計畫，將檢討與更新的結果送交管理階層審視與核定，並且將更新後之災害復原計畫通知全體相關人員。

(四) 測試與維護

制定災害復原計畫後，接下來可透過演練或測試以驗證單位所制定的災害復原計畫是否有效與可執行性。演練或測試之前應先規劃好演練或測試的腳本、目標、範圍、時程、參加人員，及預計演練或測試的項目、方法與所需的資源，以確保演練或測試之順暢。
最後，演練或測試的活動結束後應提出結果報告，報告內容應包含執行時間與地點、演練／測試過程紀錄、參加人員、演練／測試結果檢討。讓災害復原計畫能夠持續精進與及時更新，使得計畫能更符合組織的要求，藉以提升組織持續營運的能力。

三、結語

一個災情兩樣情，災害復原不可臨陣磨槍，災害復原計畫能否展現其應有的效能，主要關鍵在於作業程序、管理的落實及執行的人員。因此，組織應持續將營運持續管理、營運持續計畫及災害復原計畫融入至組織文化中，藉以獲得人員的支持與充分投入，以期讓營運持續計畫與災害復原計畫能夠發揮真正的功效。

（作者現任財團法人資訊工業策進會與行政院國家資通安全會報技術服務中心工程師）

▲Top

對公司的管理來說，除了限制外，更需要相對應的措施及破解後的因應辦法。

數位時代的員工管理

◎魯明德 / 魯晏汝

壹、前言

「你今天偷菜了嗎？」這是近來人們見面常問候的一句招呼語。隨著網路社群的蓬勃發展，人們見面從原本的「你好嗎？」「最近過得怎樣？」逐漸轉變成和網路社群有關的招呼語。

電子商務和網路社群的發展，提升了人們生活上的便利性，也拉近了朋友之間的距離，但是相對地也提高了公司經營上的風險性。員工在上班時間可能會花費過多的時間在經營網路社群或是網路購物，從而降低了工作效率；通訊軟體及存取裝置的使用，也可能導致公司內部資料的外流。身為公司的管理者，應如何透過管理的方式來約束這些員工的行為呢？

貳、電子商務與網路社群

一般電子商務依往來的型態可分為B2B（Business to Business）、B2C（Business to Customer）、C2C（Customer to Customer）三大類。B2B指的是企業對企業的電子商務型態，例如某電腦公司向其供應商購買零件生產，再將成品銷售給下游廠商等，這種公司對公司間的交易都屬於B2B；B2C則是指企業對消費者的電子商務型態，像亞馬遜網路書店（Amazon.com）、Yahoo奇摩購物中心等，這種企業透過網路將產品賣給消費者的方式都可稱為B2C電子商務型態；而C2C則是指消費者直接對消費者的電子商務型態，常見的有eBay拍賣網站等等。

至於網路社群也幾乎可說是現代人生活中不可或缺的一部分，如果想找八卦消息、尋求網友的意見與評價，就會想到PTT、Mobile01等論壇，或是網路部落格（例如無名小站、yam天空部落格）等；若是想找休閒娛樂、和朋友聯絡感情，直覺起就會想到臉書（Facebook）、推特（Twitter）等平台；想要團購的話就會想到愛合購(ihergo)、地圖日記等知名團購網站。網路社群幾乎可滿足現代人生活上的各種需求。

參、如何進行員工管理

電子商務及網路社群的發展，除了帶來生活上的樂趣及便利外，也會讓公司與公司間的營業秘密、客戶資料、訂單等，藉此透過各種管道洩漏出去；以先前某人力銀行為例，曾有員工被該公司以用MSN洩漏會員資料而解僱。

存取裝置的使用也是造成公司營業資料外流的一大因素，因此有些公司會禁止存取裝置的使用，像是主機不提供ＵＳＢ連結埠，或者是附有ＵＳＢ連結埠，但是會控管這些外部儲存裝置只能被讀取而不能被寫入，這是公司用來避免員工將公司資料放進隨身碟攜出的一種作法；但在這種不能使用存取裝置的情況下，相對地通訊軟體的管制就更顯重要了。上班時間幾乎每個上班族都會使用通訊軟體，而通訊軟體造成的問題及損害也時有耳聞，除了我們常聽到的帳號被盜造成網路詐騙事件外，更常見的是透過這些通訊軟體，直接將公司內部的資料傳送出去。

為了避免這些問題，公司可以在聘僱合約上訂定公司可以隨時監控網路通訊軟體的使用，此舉也是保障公司可以合理地監控員工；除此之外也可以設置查核點，當員工啟動通訊軟體傳輸檔案時，會自動封鎖檔案傳輸的功能，禁止員工將檔案用此方式傳送出去；另外有些公司會直接限制通訊軟體的使用，目的除了讓員工可以專心工作外，也是為了避免通訊軟體所造成的資料外洩。

此外，由於電子商務及社群網站的風行，也使員工常常在上班時間不自覺地花費太多時間在經營社群網站或是瀏覽購物、拍賣網站，所以有條件地禁止員工在上班時間瀏覽這些網站是有必要的。

何謂有條件的禁止？雖然員工來公司的本份就是認真上班，並且對公司有所貢獻，但如果限制上班時間只能瀏覽公司內部的網站而不能連結外面的網站，或是即使可以連結外面的網路，但能使用的只有Yahoo或是Goole等知名搜尋網站，恐怕會讓員工覺得公司限制太多，在朋友之間討論比較時，也會給其他人不好的印象，進而影響公司的聲譽。所以要用有條件的方式來管理員工網路的使用，例如設定在上班時間不能逛網拍、買賣股票、看YouTube、關心臉書上朋友的動態、趁人家不注意時跑去「偷菜」，或是瀏覽一些網路論壇，中午休息時間及下班後的時段才能開放這些網頁的瀏覽，如此一來不止可以提升員工的工作效率，也不會讓員工覺得公司限制太嚴格，降低員工對公司的滿意度。

肆、結論

俗話說「道高一尺，魔高一丈」，不論管理層面如何地防堵，一定都還有被破解的時候，所以對於公司的管理來說，除了限制外，更需有相對應的措施及被破解後的因應辦法，一旦造成損害時才不會損失慘重，並且也才有依據請求損害賠償，不致白白損失吃悶虧。

▲Top