從資料異地備援看風險管理

資訊室

第一章　　緒論

1.1 前言

在知識經濟時代，資訊與網路基礎建設已是企業、政府及國家永續維運的命脈。有形的土地、廠房、機器設備等資產固然重要，而資訊系統中的資訊更是需小心保護的重要資產。

台灣位處於地震帶，從 921 集集大地震、牽連最多科技公司的汐止東方科學園區大火，以及美國 911 雙子星大樓恐怖攻擊事件，暴露出企業資料”異地備援”的重要性;如何因應天災及其他不確定因素可能為資料、資訊帶來的重大危害與損失，已引起各國企業的高度重視。能充分與提前掌握資料者，除能保障客戶的資料不至流失外，亦能保有在同業間的競爭優勢並增加本身企業得以永續經營的機會。

電腦資料是許多公司對外營運的核心元素,在汐止東方科學園區大火事件中，部分受災公司，如**宏碁集團**因緊急應變得宜、**網際威信公司**平時本身已做好與總部及在香港、美國的備援工作、**建碁**公司則在火災持續惡化時，適時的利用網路成功的將資料備份至遠地，資料庫均安然無恙，均屬不幸中的大幸。

但也有其他企業因事出突然，應變不及將重要的資料備份或搬離火災現場，如高鐵配合廠商橋樑隧道設計的亞新公司，其寶貴資料慘遭毀滅，造成企業後續重新營運的重大困難。

世界著名的財經諮詢公司摩根・斯坦利在世貿中心有近 4000 名員工，在 911 事件中可以說是損失巨大。值得慶幸的是，摩根・斯坦利公司在世貿中心倒塌前十幾分鐘內,透過網路方式將所有商務資料轉移到離世貿中心數公里之遙的第二辦事處,此即異地備援之實際與有效運用。在 9 月 11 日紐約世貿中心慘劇發生之後，許多公司的商務資料在瞬間毀於一旦，而同樣遭受浩劫的摩根・斯坦利公司卻在第二天就正常運轉的秘訣。

企業主若平時將資料做好風險管理,除了平日的備份外亦做好災難備援計劃，定時將資料備份至他處，不定時作災害演練則能確保本身企業得以永續經營。就如宏碁董事長施振榮所表示的，多數受災企

業，都有投保相關產險，企業在實體資產上的損失不致太大。然而企業若因沒有做好備份工作，所需的重新製作與知識的重建，甚至復原對外的營運服務所需的時間成本與商譽的損害，才是真正龐大且難以估計的損害。

第二章　異地備援及風險管理探討

目前異地備援對於重視資料保存的企業來說已逐漸受到重視，因此認識異地備援及了解其相關的專業知識，已越趨普遍且是必備的條件；而在同地且同機備份的作法，就風險管理方面而言已稍嫌不足。因此本章將針對異地備援、異地備援類別、可能性風險、及風險控管理等相關主題作簡要之介紹。

2.1 異地備援

異地備援即是將企業內所需之資料，分開兩地存放；平時兩地之資料，可隨時做同步化動作，並且於災難發生時，能即時運轉提供服務，以便當一地的設備發生運轉問題，另一地建置的設備可以立即接手取代繼續運轉。如此一來，企業所提供的資訊服務不會因地理位置所發生的天災人禍等不可抗拒事件而中斷。

對於醫療業本身而言，有二十四小時運作的急診室、藥局、住院、護理站、掛號批價等系統，這些系統因是二十四小時運作，如果中斷將造成人力資源加重及患者等待時間加長、醫師增長看診時間，無形之中造成醫院營運成本增加，及醫療風險的增加等等。

2.2 異地備援類別

由於備援主要牽涉之關鍵設置為儲存設備，因此儲存設備將成為企業異地備援基礎架構中之主要核心。而目前大型儲存設備的主流架構為 SAN 與 NAS

1. SAN(Storage Area Network）：為區域網路儲存，採用光纖通道，以中大型架構為主，用於在固定時間內只被少數人同時存取。
2. NAS(Network Attached Storage）：為網路連接儲存，利用 IP 傳輸，若有大量用戶需同時讀取資料的環境時，NAS 儲存設備是理想選擇。

2.3 異地備援的可能性風險

2.3.1 資安風險

異地備援可能會有下列的風險

1.資料的外洩：資料在傳輸的過程中被有心或無心人士所得到。

2.資料處理的正確與完整：資料在傳送或儲存後所得結果是否與原來資料相同。

3.營運中斷：資料毀損後到還原這段時間造成企業營運中斷。

2.4.2 資安威脅

對於企業組織的資訊安全，駭客、間諜、病毒、蠕蟲、惡意破壞者和洩密者等於是企業組織必須面對的威脅；

1.病毒（蠕蟲）：儲存系統本身若無防毒程式則可能將病毒一起備份，造成備份資料皆受病毒感染。

2.洩密者（間諜）：公司員工有可能透過伺服器入侵儲存系統，截取資料。

3.電力供應不正常：若電力突然間斷掉，將導致瞬間電壓不穩，造成資料在儲存瞬間不正確。

4.不可預知的水災、火災、地震等。

5.網站入侵與攻擊：利用網站伺服器的漏洞從而取得網站之重要資訊、置換網頁或使網站停止服務。

2.4 風險管理

2.4.1 針對資安風險部份

可以使用 VPN 通道及在備援端也安裝相同之資料庫，平時設定每日進行差異性備份，在登入資料庫時也另寫一隻程式連到備援端，當有問題時立刻將連線資料庫改成備援端，如此可減少資料的外洩、縮短營運中斷時間、及確保資料正確性與完整性。

2.4.2 針對資安威脅部份

可輔導企業本身導入 BS7799 資訊安全管理，針對不同的企業特性建立一套完整的資訊安全管理系統，使企業資訊安全目標得以達成。欲達成目標，需管理面與技術面的統合，缺一不可。至於風險部份則無法完全去除，因每個企業面對不同的風險時所能承受的程度會有差異，這也就是在導入 BS7799 時，因應企業需求的不同而建議採用不同的方式。

第三章 結論

企業的目的不外乎永續經營以達成企業本身的獲利，資料可說是整個企業的命脈，有形的資產及土地可以用金錢再買回相同實體即可運作，然資料的遺失或毀損有時是金錢無法購回原來的資料且可能導致企業營運的危機。

異地備援除了能夠將資料備份在本地端及異地端，確保資料不致在同一時間同一地點因為天災或人為因素導致資料毀損，且可確保因為硬體的故障需要維修停機時的人力成本增加。然目前多數企業主都有一種心態就是不會有那麼倒楣的事發生，但我們寧願有備而不用卻不要等到事情發生時才在後悔莫及。

風險每個企業都會面對的問題，特別是醫療業每天都必須面對醫病關係的風險，但面對風險要如何管理則是每個企業主必須認真思考的問題，除了列管每天所遇到的異常事件，並且制定成知識庫做為新進人員訓練時的教材，最重要的是針對可能會發生的風險做好人員的教育訓練，因為人才是企業最重要的資產，一個企業全部都是新進人員跟一個企業都是資深員工，它們所面對的風險自然不同。

異地備援需良好的硬體搭配良好的管理制度及優秀的人力技術，如此才能免於資料受到毀損的風險進而導致企業的危機。