# 宜進實業・資通安全治理暨風險評估報告

〈摘要版〉

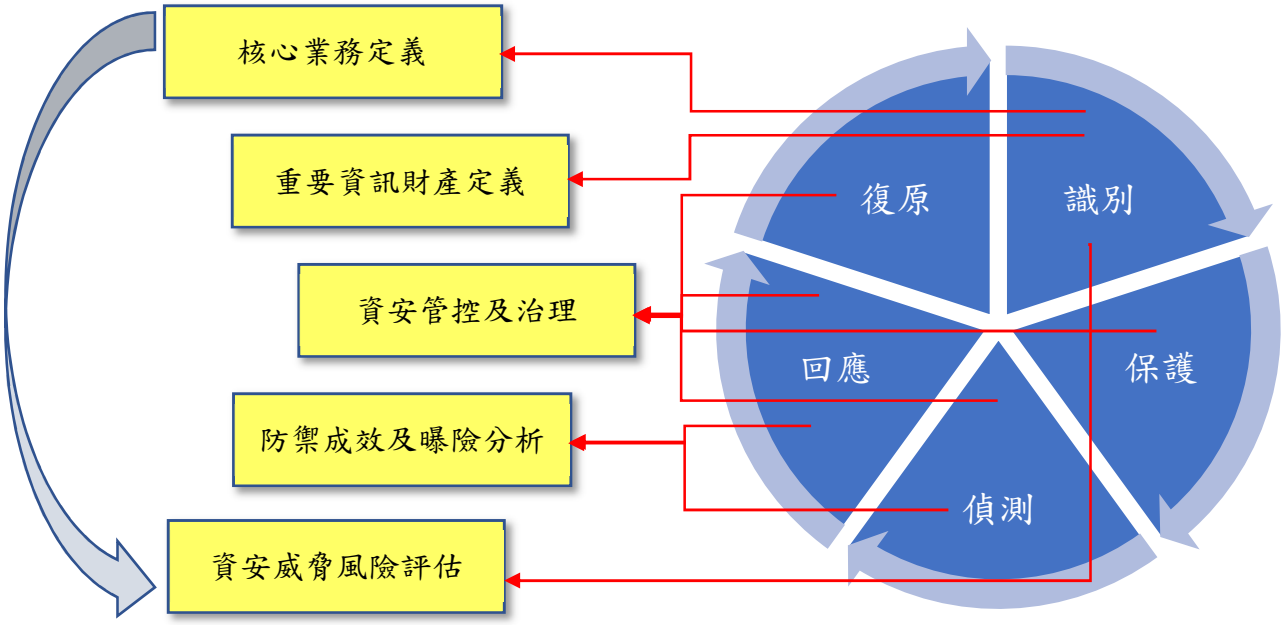
| 資料統計分析期間 | 2022 年 1 月～12 月 | 製　作　單　位 | 資 安 管 理 小 組 |
|---|---|---|---|

本公司資通安全管理事務由「資安管理小組」統籌指揮，督導資安政策之落實及資安措施之執行，協調各項資源分配，提升資安之防禦能力及抗擊韌性，建立同仁安全的資訊作業觀念，以降低整體之資安威脅及風險，並每年定期向董事會提報資訊作業之風險評估報告。

本公司的資訊安全風險評估乃針對核心業務，從資訊環境之端點、閘道到網際網路三個作業層面剖析重要之資訊財產及可能面臨的威脅及風險，再從已導入的多層次資安管控措施或防禦設備，於控制點所產生之數據，量化後綜合呈現其曝險趨勢，以使經營團隊對公司整體資訊作業的風險程度，有具體的概念及警覺，並在面臨威脅事件時能快速回應並及時採取防範作為，以維護公司資訊財產的安全性及完整性。

本資訊安全治理暨風險評估報告的架構以圖示表達如下。

| 資訊安全治理暨風險評估 | 網路安全風險生命周期 |
|---|---|



## 一、核心業務及重要資訊財產

定義核心業務 ⇨ 定義重要資訊財產 ⇨ 重要資訊財產之價值量化

1-1. 本公司之重要及核心業務說明如下：

| 重要業務<br>(◎核心業務) | 資訊管理系統/資料 | 重要性 | 資訊環境失效對營運的影響程度 | 最大可容忍之中斷時間 |
|---|---|---|---|---|
| ◎產品銷售作業 | 銷售管理系統 | 為公司持續營運之必要業務 | 中 /<br>改人工作業 | 1 週 |
| ◎原物料採購作業 | 庫存管理系統-驗收作業 | 為公司持續生產之必要業務 | 低 /<br>改人工作業 | 2 週 |
| ◎委外生產及出貨作業 | 庫存管理系統-委外送貨、委外退回作業 | 為公司持續生產之必要業務 | 中 /<br>改人工作業 | 1 週 |
| ◎財會出納作業 | 總帳會計系統、應收/應付票據管理系統 | 為公司持續營運之必要業務 | 中 /<br>改人工作業 | 1 週 |
| 內部稽核作業 | 電子文書資料檔 | 為公司治理之必要業務 | 低 /<br>改單機作業 | 3 週 |
| 行政管理作業 | 人力資源管理系統、電子文書資料檔 | 為公司持續營運之必要業務 | 中 /<br>改人工作業 | 2 週 |
| 資訊及資安管理作業 | 資訊設備之日誌、電子文書資料檔 | 確保資訊作業環境安全之必要業務 | 低 /<br>無法人工作業 | 3 週 |
| 董事議事管理公開資訊申報 | 資訊管理系統、電子文書資料檔 | 為公司治理之必要業務 | 中 /<br>改單機+外部作業 | 2 週 |

[註 1]資訊環境失效對營運的影響程度：

**高**. 會影響多個作業單位，資訊作業延遲會影響帳款之結帳或資料申報的時限，或損害公司的聲譽、形象。

**中**. 會影響 1、2 個作業單位，資訊作業延遲雖降低帳款之結帳或資料申報的時效，但仍有替代方法可協助及時完成。

**低**. 不影響其它單位作業、帳款之結帳或資料申報的時間，但仍為日常管理或主管機關要求之重要執行事項。

1-2. 為維繫上述重要業務之持續運作，在各作業層面所需的重要資訊財產列示如下：

| 作業層面 | 資產名稱 | 功能失效對**業務**的影響程度/<br>最大可容忍之中斷時間 |
|---|---|---|
| 內部網路/環境 | 伺服器(營運資料庫具 HA 架構) | 高 / 5 天 |
| | 個人電腦(Windows) | 高 / 2 天 |
| | 交換器(Switch) | 高 / 2 天 |
| | 不斷電系統(UPS) | 中 / 5 天 |
| | 機房及溫控、消防設施 | 低 / 10 天 |
| | 資料備份伺服器(NAS) | 中 / 2 天 |

| | | |
|---|---|---|
| | 資訊管理系統(程式及執行環境) | 中 / 5 天 |
| | 電子資料檔及資料庫 | 高 / 2 天 |
| | 重要作業執行人員 | 中 / 5 天 |
| 閘道 | 防火牆 | 高 / 2 天 |
| 網際網路/外部 | 電子郵件主機(採硬碟鏡射) | 高 / 2 天 |
| | 公司網站(委外設計&維護管理) | 低 / 10 天 |
| | 連外光纖線路 | 高 / 2 天 |
| | 支援服務/廠商(有定期服務/合約) | 中 / 5 天 |

[註 2]資訊設備功能失效對重要業務的影響程度：

**高**. 會影響資訊安全、作業的及時性或會使公司受到財務損失。

**中**. 不影響作業的及時性，但對營運流程或資訊安全仍有重大影響，具不確定風險。

**低**. 各項資訊作業仍能持續，為資訊或資安管理上所需，以避免突發事故衍生嚴重後果。

1-3. 為利於後續評估對資產將採取之風險因應方式及保護力道，上述重要資訊財產依 6-1. 資訊財產之價值估量表區分機密性、完整性及可用性，做較精細的價值(最高 12)估算如下：

| 資產名稱 | 與**核心業務**之依存關聯性 | 機密性(C) | 完整性(I) | 可用性(A) | 資產價值(W)=C+I+A |
|---|---|---|---|---|---|
| 伺服器(營運資料庫) | 高（各項帳款處理） | 3 | 4 | 3 | 10 |
| 個人電腦(Windows) | 高（郵件往來、文書處理） | 3 | 4 | 2 | 9 |
| 交換器(Switch) | 高（內/外網路連線） | 2 | 3 | 2 | 7 |
| 不斷電系統(UPS) | 中（避免市電中斷） | 1 | 2 | 2 | 5 |
| 機房及溫控、消防設施 | 低（提供穩定的作業環境） | 3 | 1 | 1 | 5 |
| 資料備份伺服器(NAS) | 中（提供共用目錄、備份） | 3 | 3 | 2 | 8 |
| 資訊管理系統 | 高（各項帳款處理） | 3 | 3 | 1 | 7 |
| 電子資料檔及資料庫 | 高（業務資料來源） | 4 | 4 | 2 | 10 |
| 重要作業執行人員 | 高（執行各項作業） | 3 | 3 | 1 | 7 |
| 防火牆 | 高（防禦、對外網路連線） | 4 | 4 | 2 | 10 |
| 電子郵件主機 | 高（利害關係人溝通） | 4 | 4 | 2 | 10 |
| 公司網站(委外設計&維護管理) | 低（公司治理、利害關係人溝通） | 1 | 2 | 1 | 4 |
| 連外光纖線路 | 高（對外網路連線） | 2 | 4 | 2 | 8 |
| 支援服務/廠商 | 中～高（緊急維護支援;伺服器的關聯性較高） | 3 | 3 | 1 | 7 |

## 二、資通安全管控及治理

資安管理分類 ⇨ 管控措施及執行說明 ⇨ 管控措施之成熟度自評

本公司對資安風險之管控以內部控制為根基，參考外部實例或廠商建議而持續改進，所採取之管控措施(如下表)乃衡量經營管理階層對營運宗旨與企業價值之共識，針對核心業務及重要工作之發展進程，依 ISACA 國際電腦稽核協會台灣分會之"資通安全公司自我檢查表"的 10 個分類於每年定期自我評估及分析後，依據其中風險性較高的部份進行檢討及擬具改善措施，從系統面、技術面、程序面，對已知之威脅採取適當之處理方法，對潛藏之威脅盡可能予以事前分析及鑑別，以保護公司資訊財產的機密性、可用性及完整性，避免遭受各種威脅及降低可能的危害或損失，以提升本公司承受外部攻擊之防護能力及應變彈性，減緩衝擊等級及降低可能造成的損害，妥善因應風險。

| 項次 | 資安管理分類 | 重要管控措施 | 執行頻率 |
|---|---|---|---|
| 1 | 資訊安全政策 | ‧明定資安組織、權責及事件之通報、處理綱要。 | 檢視 1 次/年 |
| | | ‧定期審查、修訂資訊安全政策。 | |
| | | ‧資通安全治理執行成效及風險評估，並向董事會提報。 | 彙編 1 次/年 |
| | | ‧配合政府法規及國際相關準則，研議資訊安全管理相關辦法，規範內部執行事項。 | 不定期 |
| 2 | 建立資訊安全組織 | ‧設資安管理小組及個人資料保護小組，定期開會討論資安相關事宜。 | 至少 1 次/半年 |
| | | ‧訂立資安事件之緊急應變處理及回報程序，由資安管理小組統籌管控。 | 不定期 |
| | | ‧派員參與資訊安全之研討會及相關課程。 | |
| 3 | 人員安全與管理 | ‧內部控制制度定義資訊人員、使用者之作業權限劃分，及人員異動、離職之作業準則。 | 檢視 1 次/年 |
| | | ‧定期執行作業權限複核。 | 至少 1 次/半年 |
| | | ‧資訊管理系統的密碼實施複雜性原則檢查，定期要求變更。 | 變更 1 次/半年 |
| | | ‧定期普查個人電腦，防止公器私用。 | 執行 1 次/年 |
| 4 | 資產分類與控管 | ‧核心業務之資訊軟、硬體資產定期盤點及列冊管理。 | 執行 1 次/年 |
| | | ‧重要的伺服器、資訊系統每年簽訂委外維護合約，確保持續運作。 | 1 次/年 |
| 5 | 實體及環境安全管理 | ‧專用電腦機房具獨立空調、溫度自動控管及消防設施。 | 每日檢視 |
| | | ‧使用不斷電系統保障電源之緊急供應，並定期保養、檢測。 | 保檢 1 次/年 |
| | | ‧伺服器及個人電腦安裝防毒軟體，重要職務之電腦，每日定時備份，其備份份數至少二代。 | 每日、每週執行 |
| | | ‧營運資料庫採雙主機即時備援，每半年定期模擬事故演練後輪替運作。 | 切換 1 次/半年 |
| | | ‧對重要伺服器或網路設備定期弱點掃瞄。 | 執行 1 次/週 |
| 6 | 通訊與操作管理 | ‧電子郵件主機具自我防護及保存稽核之功能，並在雲端使用 Hinet 郵件守門員過濾可疑、惡意郵件。 | 每日執行 |
| | | ‧設置閘道防火牆並分析紀錄，並使用趨勢雲端防護軟體分析、記錄上網行為，即時防堵內、外部異常行為。 | 每日檢視 |
| | | ‧使用 Hinet 資安艦隊之防駭守門員、先進網路防禦等服務，擴展防禦的廣、深度，防堵內、外之攻擊。 | 每日執行 |
| | | ‧DDOS 分散式阻斷防護機制，過濾、清洗電路流量。[必要時用] | 連續 3 天/年 |
| | | ‧即時宣導資安事件、通告或案例，提升防護意識。 | 至少 1 次/季 |

| | | | |
|---|---|---|---|
| 7 | 存取控制 | • 電子檔資料依部門、個人設定存取權限。 | 每日執行 |
| | | • 對外連線作業申請需經部門主管同意及副總級以上主管核准。 | 有需求時執行 |
| | | • 電子郵件區分權限，不須對外連絡者僅能內部寄信。 | 有需求時執行 |
| | | • 人力資源系統於讀取個資時，自動記錄存取軌跡。 | 每次存取時執行 |
| 8 | 系統開發與維護 | • 自行開發、維護的資訊管理系統，在規劃分析時主動將安全需求納入設計考量，防範外部的侵入篡改，並限制特權帳號之使用對象。 | 有需求時執行 |
| | | • 資訊管理系統的程式在修改前留存備份，於程式開頭註記修改資訊；修改後，經權責主管複核後上線。 | |
| | | • 系統開發文件限制存取權限，非開發人員不得編輯。 | |
| 9 | 永續運作之計畫管理 | • 營運資料庫主機每半年定期模擬事故演練、測試。 | 演練 1 次/半年 |
| | | • 重要設備訂立緊急應變計劃，供發生重大資安事件時遵循及應變。 | 需要時執行 |
| | | • 各項防護措施之數據指標化，供評估運作之風險及研討因應措施。 | 每日 |
| 10 | 內部稽查及其它 | • 每年電腦普查時公告公司軟體所授權之範圍，授權以外之軟體則要求移除或提供授權證明；由平日異動及普查結果，更新核心業務之資產狀況。 | 普查 1 次/年<br>資料隨時更新 |
| | | • 資訊單位定期自評資訊作業環境安全。 | 自評 1 次/年 |
| | | • 稽核單位定期自評資訊控制作業。 | 自評 1 次/年 |
| | | • 內部稽核人員及會計師團隊每年定期稽查資訊控制作業之執行情形。 | 每年至少一次 |

對上列管控措施在執行上的達成度或完整度評量，共分為五級的成熟度：完整、良好、尚可、待加強、差，2022 年度經資訊單位於 2022 年 12 月完成自評為”尚可”，自評報告經資安主管及總經理核閱，並依據風險性較高的部份進行檢討及擬具改善措施。

## 三、資安之防禦成效及曝險分析(定量分析)

防禦數據統計 ⇨ 風險量化 ⇨ 歷史風險趨勢及重點說明

3-1. 本公司自 2021 年 7 月起陸續導入 Hinet 資安艦隊之防護解決方案，以便即時防堵網路作業的異常行為，其定期產生之防護報告均明確呈現**已阻擋**之威脅數目或風險程度，雖缺乏業界之整體指標做為比較，但經長期累積其統計數據，再將此基礎資料依風險程度予以量化，轉換為資安的曝險程度指標，以表達對既有風險之管控成效，並做為日後改善措施之參考。

3-2. 風險量化的方式乃以資安防護紀錄資料中對資安層面較能呈現威脅程度的關鍵項目做為量化因子，依風險等級之高、中、低分別計算各月的平均數，再乘以不同權值後合計為風險值。

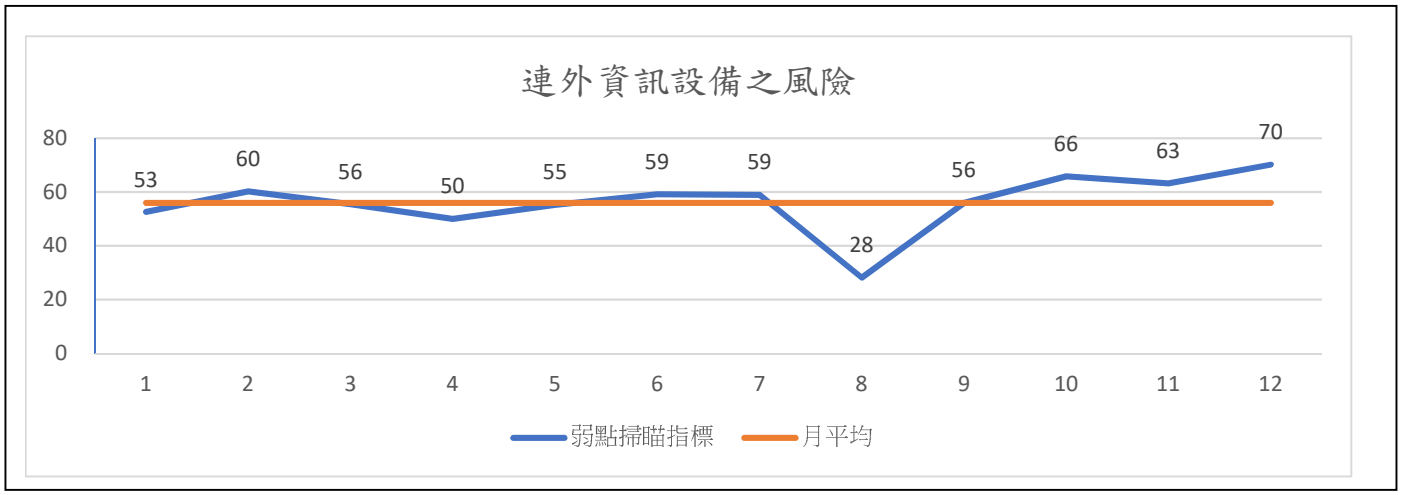
| 防護措施 | 功能說明 |
|---|---|
| 弱點偵測 | 以高度精確和極低的誤報率的掃描能力和功能，全面性掃描防火牆及郵件伺服器的所有網路埠及系統上的弱點。 |
| 企業防駭守門員 | 從外部網路端直接阻擋殭屍網路(Botnet)、惡意中繼站(C&C)、勒索軟體等惡意連線，降低受駭風險。 |

| | |
|---|---|
| 先進網路防禦系統 | 阻絕來自 Internet 的駭客攻擊，包含 IPS 防止入侵攻擊、隔絕網路病毒、阻擋惡意連線及上網內容過濾等防護功能，減少攻擊封包進出企業內部，降低企業受駭的機率；另以應用程式控管、國別流量控管、檔案傳輸控管等進階功能，進一步保障企業資訊安全。 |
| 郵件守門員 | 利用多層式偵測技術與來自全球規模最大的民間威脅情報網路的洞察力，高效率且精準地防禦新型與複雜的電子郵件威脅，例如、魚叉式網路釣魚攻擊、勒索軟體和商務電子郵件入侵（簡稱 BEC），提供企業最佳的電子郵件安全防護。 |
| NGFW PA 防火牆 | 除了一般防火牆的功能，另結合三合一防禦功能：TP.入侵防護及防毒、UF.網頁過濾、WF.雲端沙箱，從 ACC(應用程式控管中心)的頁籤，可檢視網路流量、威脅活動、封鎖的活動、通道活動。 |

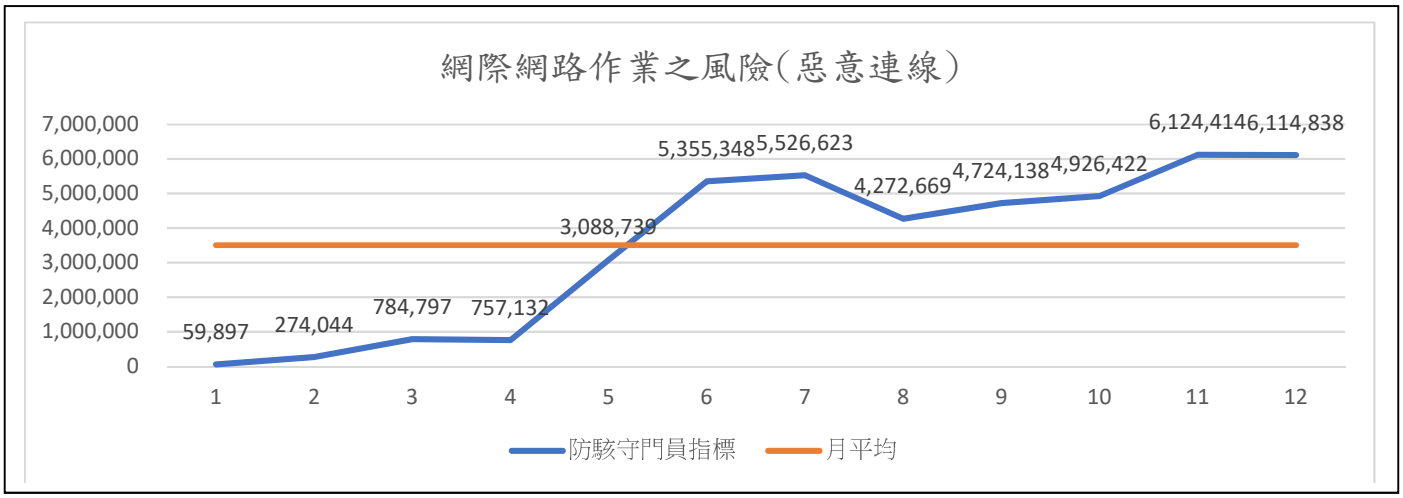
3-3. 月風險值=量化因子之（低風險數月平均值x1)+(中風險數月平均值x2)+
(高風險數月平均值x3)[+(嚴重風險數月平均值x4)]

採用 2022 年之統計數據(請參考 6-6.資安防護措施之年度統計數據)，依量化因子的風險等級之高、中、低予以轉換計算後，以折線圖呈現年度的曝險趨勢如下：

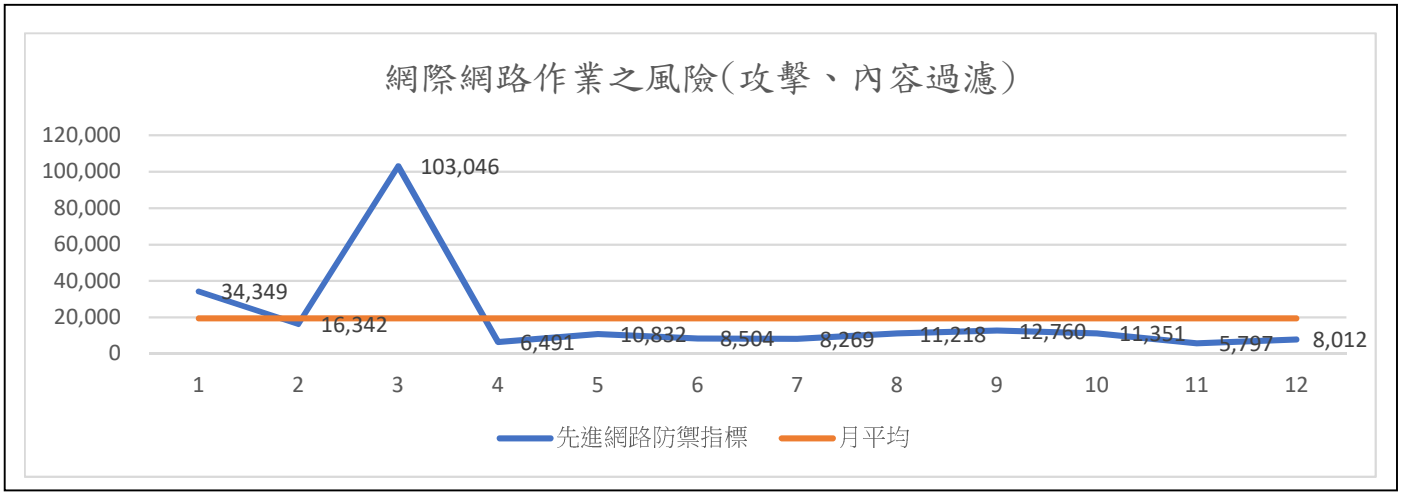
3-3-1.弱點掃瞄：連外設備之弱點風險趨勢列示如下；所列示之弱點，多為對外提供相關服務時，所必須開放的連接埠，為必須承擔之風險。



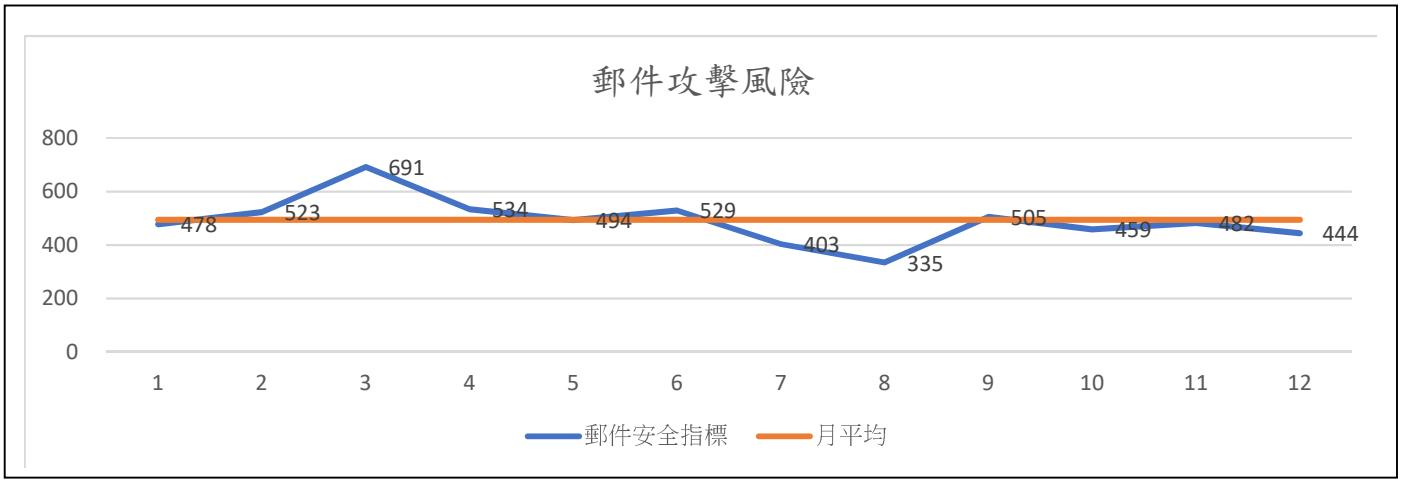

3-3-2.防禦守門員：在網際網路的連線風險趨勢列示如下。



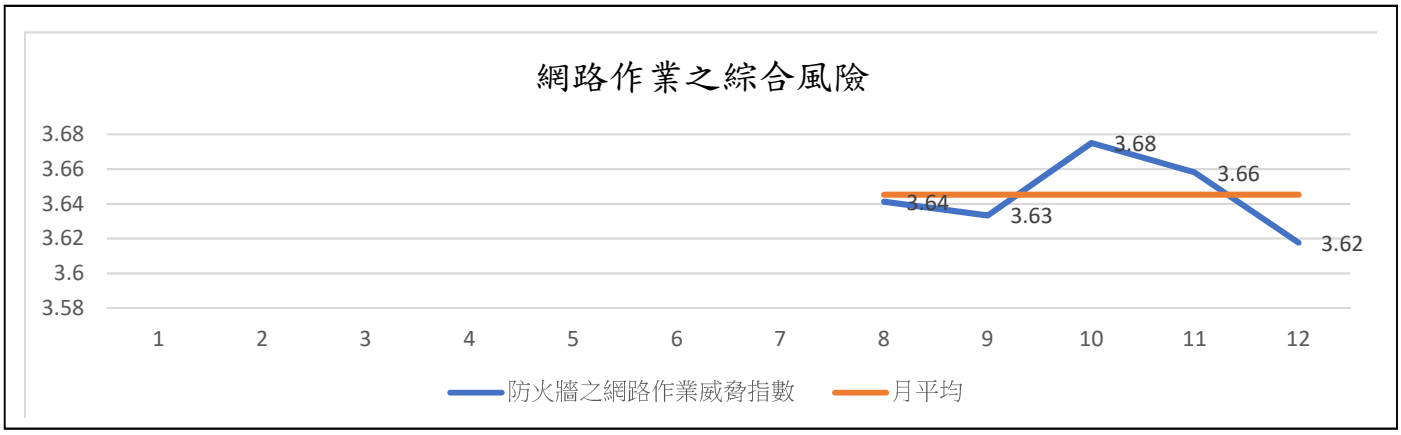
3-3-3. 先進網路防禦系統：在網際網路作業時遭受攻擊的風險趨勢。



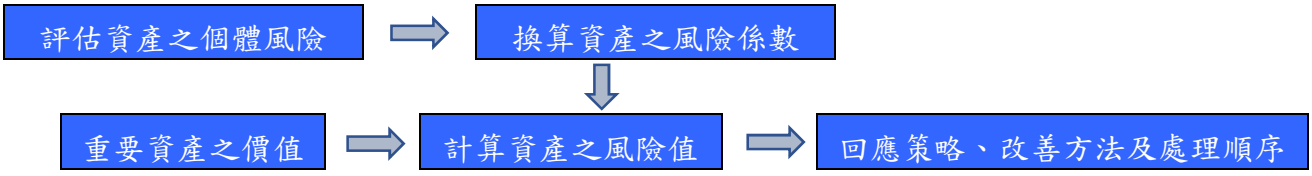

3-3-4. 郵件守門員：電子郵件往來的作業風險趨勢。




3-3-5. 防火牆(PA-220)資安指標：各項應用程式於網路執行之綜合風險趨勢。



## 四、資安威脅之風險評估(定性評估)




4-1. 對於未來的資通訊的安全風險分析，本公司乃針對資訊財產當遭受到威脅時，在考慮資訊環境經控管後，假設資產發生功能失效時，其脆弱性對公司營運上產生之風險水準評估；關於風險評估項目、計算公式及相關事項說明如下：

4-1-1. 資安風險評估乃考量資訊財產的價值、威脅-弱點事件之可能性及衝擊性等項目，資產價值之評估標準請參考 6-1.資產價值評估量表，各威脅事件的可能性及衝擊性之評估標準請參考 6-2.可能性及衝擊性評估量表。風險值(VaR：Value-at-Risk)乃依據威脅發生之可能性及衝擊性程度評估給分，所得風險值為已採取回應管控措施之後的殘留風險(Residual Risk)，而非資產之固有風險。

4-1-2. 進行評估之資訊財產，可能面臨之威脅-弱點事件分為下列五類，請參考 6-3.威脅及弱點對應表；因各類資產之威脅事件項數不一致，在評估完 6-4.單一資產的個體風險值($R_T$)，需再除以資產所屬類別的總風險值(R)，換算為風險係數($R_C$：Risk coefficient)，以取得相同的比較基礎，之後再計算風險等級。

資產類別之總風險值(R)＝威脅項數×可能性最高值 3×衝擊性最高值 3 (如下表)

資產風險係數($R_C$)＝該資產個體風險值($R_T$)÷所屬資產類別之總風險值(R)

| 資產風險類別 | 說　　明 | 威脅項數 |
|---|---|---|
| H.實體資產風險 (**H**ardware risk) | 包含缺少實體安控或環境監控不足等所產生之風險。 | 18 |
| S.軟體資產風險 (**S**oftware risk) | 包含系統設計、維護、操作不當等所產生之風險。 | 18 |
| I.資訊資產風險 (**I**nformation data risk) | 包含資料、文件之建立、維護、控管、傳遞不當等所產生之風險。 | 10 |
| T.支援服務資產風險 (**T**echnical support services risk) | 包含容量不足或維護之不當等所產生之風險。 | 3 |
| E.人員資產風險 (**E**mployees risk) | 包含因人員有意或無意行為、安全訓練不足等所產生之風險。 | 12 |

4-1-3. 資產價值(W)＝資產之機密性(C)＋完整性(I)＋可用性(A)，三個性質各區分四個等級給分，最高為 12 分，此資產價值已於第 1-3 節估算完成。

4-1-4. 資產風險值(AR)＝資產價值(W)×資產風險係數($R_C$)

以資產風險值對照下列風險等級，當資產風險為高風險時，應填寫風險之因應或改善對策，並由資訊或相關單位於年度計畫中提報專案進行改善作業。

| 風險等級(Risk Level) | 低風險 | 中風險 | 高風險 |
|---|---|---|---|
| 資產風險值(Asset Risk) | **0.1~4** | **4.1~8** | **8.1~12** |

4-1-5. 風險之應對策略分為下列四種方式，詳細說明請參考 6-5.風險應對策略。

**Avoid.規避**：迴避風險發生的可能性，以完全消除威脅。

**Transfer.轉移**：將風險由原資產轉嫁由第三方負責承擔，部分的風險仍需由己方承擔。

**Mitigate.減輕**：在執行前或執行中降低威脅發生的機率或影響，預防損失發生及降低損失的嚴重性。

**Accept.接受**：必須使用資產或無其他適合策略時，承擔不願或無法轉移的風險。

4-2. 依據上述評估方法，針對資訊財產進行分類及估算風險值於 6-4.資訊財產風險評估表，評估結果彙整如下表：

| 資產分類 | 資產名稱 | 資產價值 /個體風險 | 風險係數 /資產風險 | 風險等級 /回應策略 | 因應/改善對策 | 處理順序 |
|---|---|---|---|---|---|---|
| H. 實體資產 | 伺服器(營運資料庫) | 10 / 36 | 0.22 / 2.2 | 低 / 規避 | 建立異地備份及雲端虛擬主機。 | 優先 |
| | 個人電腦(Windows) | 9 / 33 | 0.20 / 1.8 | 低 / 轉移 | 提供遠端連線作業及雲端虛擬主機。 | 優先 |
| | 交換器(Switch) | 7 / 28 | 0.17 / 1.2 | 低 / 減輕 | 以備品因應。 | 高 |
| | 資料備份伺服器(NAS) | 8 / 33 | 0.20 / 1.6 | 低 / 減輕 | 建立異地備份機制。 | 高 |
| | 防火牆 | 10 / 31 | 0.19 / 1.9 | 低 / 轉移 | 以備品因應。 | 優先 |
| | 電子郵件主機 | 10 / 35 | 0.22 / 2.2 | 低 / 規避 | 以鏡射硬碟或舊版郵件主機接替。 | 優先 |
| S. 軟體資產 | 資訊管理系統 | 7 / 26 | 0.16 / 1.1 | 低 / 規避 | 從另一伺服器建立作業環境，回復資訊系統。 | 高 |
| I. 資訊資產 | 電子資料檔及資料庫 | 10 / 22 | 0.24 / 2.4 | 低 / 規避 | 從另一伺服器建立作業環境，回復資訊系統。 | 優先 |
| T. 支援服務資產 | 不斷電系統(UPS) | 5 / 3 | 0.11 / 0.6 | 低 / 轉移 | 暫時使用市電。 | 普通 |
| | 機房及溫控、消防設施 | 5 / 3 | 0.11 / 0.6 | 低 / 轉移 | 使用其他散熱設備(如電風扇、手持式滅火器)。 | 普通 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 公司網站(委外設計&維護管理) | 4 / 3 | 0.11 / 0.4 | 低 / 轉移 | 以電話、傳真、租賃式網站暫代。 | 普通 |
| | 連外光纖線路 | 8 / 3 | 0.11 / 0.9 | 低 / 減輕 | 採用多元連線方式(如 4G/5G)。 | 普通 |
| | 支援服務/廠商 | 7 / 6 | 0.22 / 1.6 | 低 / 轉移 | 平日保持多廠商之採購政策，維繫服務關係，保持緊急聯絡之管道。 | 優先 |
| E.人員資產 | 重要作業執行人員 | 7 / 21 | 0.19 / 1.4 | 低 / 轉移 | 落實工作輪調及建立代理人制度，運用人力派遣。 | 高 |

## 五、結論

5-1. 本公司於 2022 年度之重大資安事件統計如下，對業務及財務並未產生影響。

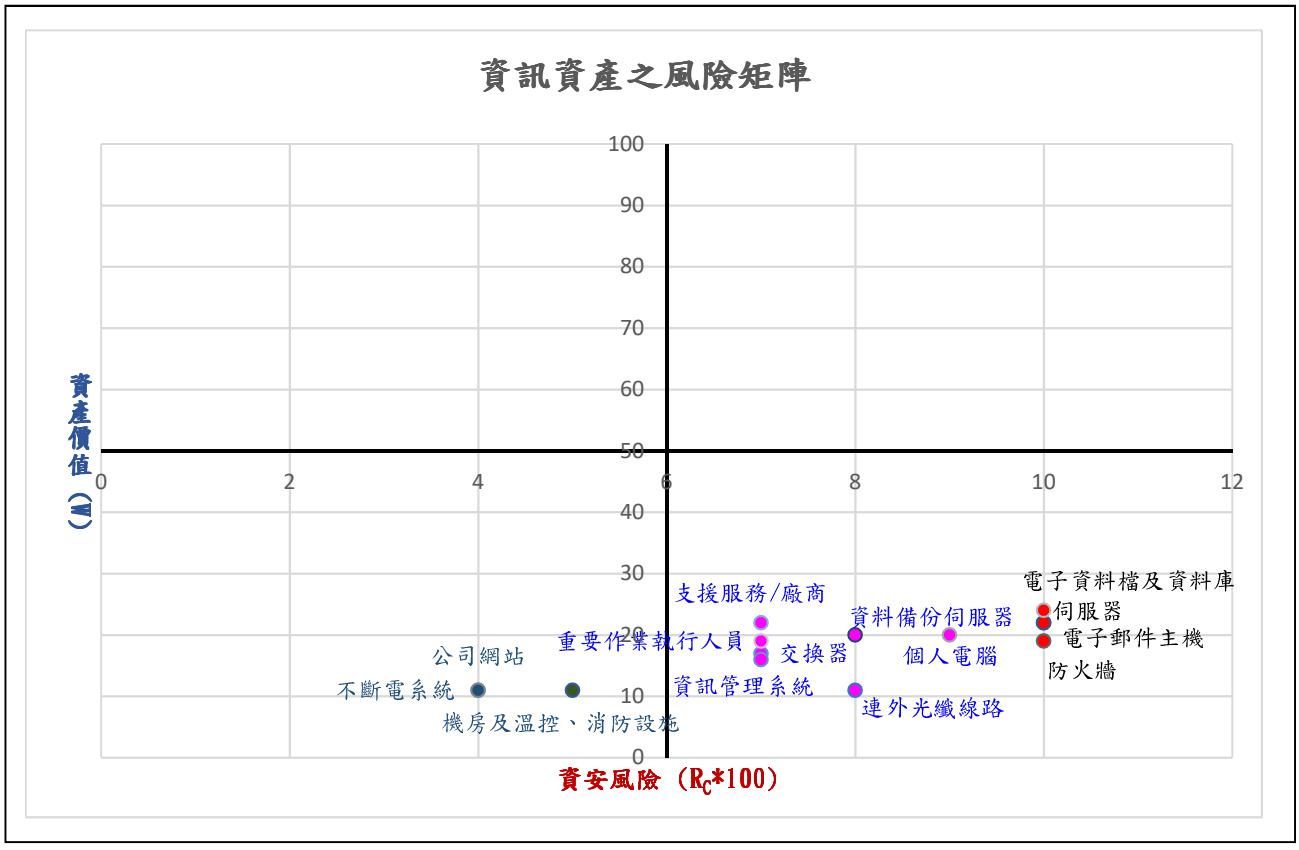
| 月份 / 統計項目 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 月平均 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 營業額（單位:百萬元） | 385 | 370 | 452 | 419 | 408 | 353 | 310 | 365 | 349 | 360 | 281 | 299 | 335 |
| 停工一日之損失營業額 | 12 | 13 | 15 | 14 | 13 | 12 | 10 | 12 | 12 | 12 | 9 | 10 | 11 |
| 發生重大事件次數 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 重大事件之損失天數 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 重大事件之損失金額 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 重大資安事件年度損失 | $0 | | | | | | | | | | | | |

5-2. 從已採取的各項資安防護措施之 2022 年風險量化數據得知，本公司之資訊環境具一定程度之網路作業風險，各月份之風險值，除了在網際網路的連線風險逐月攀升和有少部份之偏離之外，其餘大多趨近於平均值，起伏多在一個標準差之內，表示外在的網路連線或網頁內容雖有愈來愈多的偽裝或未採用安全的設計技術，但各項防護措施均能發揮其功效，阻擋各種不當的網路作業，再加上內部控制上的各類管控作為，使整體風險控制在穩定的狀態；基於上述評估結果，認為本公司於 2022 年度在資訊安全維護效果、防禦措施之可靠性、資訊內部控制作業程序和方法之設計及執行係屬有效，其能確保資訊安全政策之落實。

5-3. 對於未來的資通安全風險，雖評估後整體資安處在低風險的位階，但對節節升高和變異精進的資安威脅，謹抱持”只有更好、沒有最好”的防禦心態，劍及履及的積極做好防範措施；以下從 6-4.資訊財產風險評估表，再個別分析發生可能性、影響性及資產風險相對偏高之項目如下，做為短期上應關注的焦點。

| 資產風險類別 | 發生可能性偏高的威脅 | 影響性偏高的威脅 | 風險偏高的資產 |
|---|---|---|---|
| H.實體資產 | 1.地震<br>2.暴風雨/颱風 | 1.火災、破壞(含戰爭)<br>2.水災、地震<br>3.未授權存取資料、技術失能、偷竊 | 1.個人電腦<br>2.伺服器(營運資料庫)<br>3.電子郵件主機 |
| S.軟體資產 | 1.軟體程式錯誤<br>2.竄改或任意變更 | 1.竄改或任意變更<br>2.未授權連線存取<br>3.入侵、社交工程 | |
| I.資訊資產 | 作業人員或使用者錯誤 | 1.火災<br>2.作業失能<br>3.未授權存取資料 | 電子資料檔及資料庫 |
| T.支援服務資產 | 中斷 | 中斷 | |
| E.人員資產 | 社交工程 | 1.未授權存取資料<br>2.作業人員或使用者錯誤<br>3.破壞、竄改或任意變更 | |

5-4. 從 2-4. 各類資訊財產的價值及未來遭受之威脅風險分析，導出下列風險矩陣，對第四象限中價值及對比風險偏高的資產仍應投入高度的控管。



5-5.美國國家標準與技術研究所(NIST)的網路安全框架(CSF: Cybersecurity Framework)明確定義網路安全風險生命周期為識別、保護、偵測、回應到復原，本公司從系統面建立符合實務之管控制度，從技術面導入可靠且實用之防禦方案，從程序面確實而穩健的監控查核，以落實資安政策之目標，期使資安的脈搏處在穩當且堅韌的頻率中，讓資安風險的生命周期維持良好循環；在面對錯綜複雜、難以預期的資安風險，既有因應方法絕非萬靈丹，但回應風險的策略和方法永遠不嫌多也不嫌晚，未來將加強異地備份機制，及投入評估「託管式偵測及回應」(MDR：Managed Detection and Response)，希望藉由資安委外服務的輔助，由資安的專家提供威脅追蹤及應變諮詢，協助監控網路、分析及回應各種資安事件，即時攔截、阻禦威脅，消除處理上的盲點，以使資安防護措施更加周全和即時。

## 六、附件(略)

6-1.資訊財產之價值估量表

6-1-1.機密性(C)量表

6-1-2.完整性(I)量表

6-1-3.可用性(A)量表

6-2.資安風險之可能性及衝擊性評估量表

6-2-1.可能性量表

6-2-2.衝擊性量表

6-3.資訊財產之威脅及弱點對應表

6-3-1.實體資產(**H**ardware)

6-3-2.軟體資產(**S**oftware)

6-3-3.資訊資產(**I**nformation data)

6-3-4.支援服務資產(**T**echnical support services)

6-3-5.人員資產(**E**mployees)

6-4.資訊財產風險評估表

6-5.風險應對策略

6-6.資安防護措施之年度統計數據

6-6-1.弱點掃瞄統計表

6-6-2.防駭守門員統計表

6-6-3.先進網路防禦統計表

6-6-4.郵件守門員統計表

6-6-5.PA 防火牆 ACCRiskFactor