聯博投信

2022 年度持續核心營運系統及設備資源與落實於年度預算或教育訓練之項目

1. 2022 年度核心營運系統及設備評估報告摘述

聯博台灣核心營運系統及設備係使用集團資訊系統，相關資訊安全除遵循我國法規規定，並符合集團相關政策及程序。綜觀關鍵風險指標，網路威脅的程度在不斷增加， 2022 年在全球和台灣地區發生兩起重大事件：

(1) 俄羅斯和烏克蘭之間的衝突

為因應俄羅斯與烏克蘭之間的衝突和網路戰威脅，聯博的資訊安全部門於 2022 年 3 月宣布內部緊急狀態。如果公司直接或間接成為破壞性網路攻擊的目標，可進一步部署應急措施。

聯博將 2022 年網路安全威脅等級提升至”高風險”，以反映網路威脅的顯著增加，包括：

- 2022 年 2 月俄羅斯入侵烏克蘭與網路戰威脅
- 中國、台灣和美國不斷演變的地緣政治風險以及網路戰的威脅。
- 雙重和三重勒索贖金軟體攻擊。
- 有心人士利用未被發現的軟體缺陷。
- 利用釣魚電子郵件和釣魚簡訊向無戒心的員工發送惡意軟體。

(2) 美國眾議院議長南希佩洛西於 2022 年 8 月訪問台灣

佩洛西訪問期間和訪問後一個月內，台灣發生了大規模網路攻擊事件，便利商店及火車站電視螢幕遭駭客入侵，顯示出反佩洛西的字樣，多個台灣政府網站亦受到網路攻擊。台灣數位發展部表示，該期間對台灣政府單位的網路攻擊量超過了 15,000 gigabits，是之前每日記錄的 23 倍。

聯博的網路安全、持續營運和資訊部門持續與資訊安全相關廠商合作，確保聯博的資訊安全裝置不斷更新以因應最新的威脅，並啟動加強版安全控管，以減少聯博的網路被攻擊面。聯博投信於 2022 年無發生重大資訊安全事件，整體集團的網路安全效能和績效指標均在預期範圍內運作。

在持續營運面向，公司採計畫、測試、完備三大步驟強化持續營運韌性，本年度執行情形如下:

- 計畫：與所有業務單位和高階主管進行資訊服務長期中斷之相關風險因應計畫。
- 測試：執行年度災難復原測試、網路安全桌面演習以及針對資訊服務中斷首日因應計畫的情境模擬進行測試演習。

- 完備：確認隔離關鍵系統和資料以增強持續營運韌性的計畫，並再次聚焦於公司高階主管和業務單位負責人的桌面演習。

2. 核心營運系統及設備與相關費用

(1) 核心營運相關系統及設備如虛擬桌面基礎設施(VDI, Virtual Desktop Infrastructure systems), 伺服器及儲存設備等。

(2) 聯博台灣 2022 年度相關維護費用共計新台幣$1,674,000。

3. 資訊安全教育訓練

聯博台灣於 2022 年 4 月舉辦防範網路釣魚電子郵件教育訓練，強化員工辨識及防範網路釣魚郵件之意識與能力，全體員工皆完成線上課程及測驗。

4. 持續營運與資訊安全演練

(1) 聯博在全球 (包括台灣)執行和完成了 26 次持續營運演習和測試。

(2) 證券暨期貨市場電腦緊急應變支援小組(SF-CERT) 111 年度資安事件應變桌面演練(2022/03/18)

(3) 證券暨期貨市場電腦緊急應變支援小組(SF-CERT) 111 年度電子郵件社交工程演練 (2022/6/20 ~ 2022/6/24)

(4) 證券暨期貨市場電腦緊急應變支援小組(SF-CERT) 111 年度資安通報演練 (2022/08/04)

(5) 證券暨期貨市場電腦緊急應變支援小組(SF-CERT) 111 年度資安事件應變桌面演練(2022/11/17)

(6) 聯博台灣電子郵件社交工程演練(2022/12/05 ~ 2022/12/09)