堡達實業股份有限公司

113 年資通安全執行情形報告

一、 資通安全組織架構

本公司於 112 年設置資訊安全專責主管及 1 位資訊安全人員，處理本公司資訊安全相關政策制定與推動計畫。並每年最少一次資訊安全主管於董事會議中報告本公司重大資安議題或重大事件執行規劃說明。

二、 本公司網路防火牆防毒軟體流量說明。

1. 本公司連入軟體情況

113 年 1 月本公司防火牆至 11 月底，本公司應用程式目前以加密網頁瀏覽為主，因應時代的演化與進步雲端服務正在增長，本公司資料安全存取採取私有雲方式，而系統流量存取雲端服務 apple 的 icloud 個人手機備份流量。全年增長都在合理範圍。其次需注意為 Line 其它服務正在增長，因 Line 通訊為目前常用通訊軟體內容包含圖片，影片等等…目前暫不影響本公司網路流量。但未來如持續增長需額外注意。

2. 本公司 SSL VPN 外部連入

疫情結束後，下半年關閉不必要的使用帳號後，僅外出業務部門使用，因服務資料僅能接入本公司系統與電子簽核資料，與 NAS 私有資料，如下流量為全年度正常流量。

3. 2024 年異常攻擊狀況

113 年本公司未收防火牆未收到其它異常攻擊情形。本公司保持不挑釁，不高調並與台灣電腦網路危機處理協調中心保持最新駭客攻擊手法資訊，以加強本公司防火牆規則建立。

4. 防毒軟體狀況說明

目前本公司採用趨勢 Apex One 採以主動式行為監控，目前多數防堵為不明網站為主要，主要避免使用者進入到高風險網站，可以降低詐騙，中毒與被植入木馬等風險。

5. 作業系統更新異常

Win10，Win11 系統更新近期常出現更新後系統卡住不動問題，為作業系統更新後改寫了系統資訊，以致作業系統當機，已通知使用者在系統更新後依系統要求執行重新開機處理。

三、 113 年資通安全執行情形

1. 113/01 以 E-mail 方式進行本公司海內外員工資通安全宣導。
2. 113/04 備份系統還原演練(三重異地還原)。
3. 113/03 公司主機汰換與資料清除作業。
4. 113/08 主機報廢，儲存裝置移除並格式化。
5. 113/08 召開資訊安全委員會會議。
6. 113/09 申請並加入台灣電腦網路危機處理暨協調中心(TWCERT/CC)。
7. 113/10 參加資安事件處理的準備與作業研討會。
8. 113/10 於公司朝會向員工宣導反詐騙，資訊詐騙等案例分享。

四、 本公司資安事件

113 年 1-10 月

1. 資安外洩：0 件
2. 系統異常如 ddos 攻擊：0 件
3. 設備異常影響公司運作：1 件

資安事件說明：

本公司 VPN 中華電信線路中斷已正常切換備援，報修多次中華電信建議申請直接申請光纖。多次報修且中華電信已更換超過三次設備，本公司評估為線路問題，而非中華電信數據機問題，但中華除了更換光纖，無其它解決辦法。經報修中華至本公司場勘拉光纖可能性，第三次報修場勘後無需更動裝潢，即刻升級施工處理。

五、 總結

113 年本公司於 9 月份加入 TWCERT(台灣電腦網路危機處理暨協調中心)組織，並取得情資分享，利用取得的情資來增加本公司防火牆強度。

今年度本公司資訊安全營運相對穩定，唯獨 113 年下半年度，因中華電信設備問題造成與海外 VPN 連線中斷，對應備援機制直接啟動，因此不影響海外使用者輸入系統與出貨異常狀況，其應對狀況已加入評估並於 113.08.27 召開資訊安全會議討論處理方式，並經上級主管同意針對該事件與總務單位取得後續必要之合作，得以順利跨部門溝通並解決該狀況。

本公司不定期宣導反詐騙，督導同仁遵循資安規範，在無法判斷郵件是否安全時，請求資訊部協同進行判斷，多數非相關業務訊息已有自行查證之習慣。

2024 年並無違反資通安全、造成本公司資訊或客戶資訊洩漏及罰款等重大資安事件發生。

本年度已於113年12月18日向董事會報告資通安全風險管理之落實執行情形。