持續交付能力是達和環保服務營運的基礎，因此我們致力於提供符合機密性、完整性及可用性的產品和服務。為成為業界第一流企業，應用並導入國際資安框架ISO 27001、NIST CSF以及持續強化各項安全管控措施，以提供高度資安防護能力，這是提供優質服務的基石。因此，我們持續從點線面評估資訊安全防護機制，研擬各種技術組合，採用縱深防禦及安全設計原則，從管理、資料、端點、應用、網路、第三方供應、BC/IR、情資整合與聯防等8個面向進行層層防護，降低風險發生機率；經成本效益評估，採取適當管理手法，將風險影響降低至組織可接受水平內並持續監控殘餘風險，同時透過國際驗證和紅隊演練等第三方機構來協助檢視和升級系統防護，增加企業資安韌性。

相關資安投資如下:

1. 辨識類: 資安治理必須先有良好且易於遵循的管理框架及專業資安人員投入，OO聘請外部顧問協助，建立適合組織業態之資安政策與框架，同時購買資產盤點管理系統，進行盤點與找出各資產及風險擁有者進行風險識別最後導入弱掃系統進行威脅識別、分析並做為風險處置依據，2022資安識別類投入NT$ X,XXX,XXX
2. 保護類: 藉由上述識別出之資產，依處理資料之機敏程度進行分類，並透過強化實體安全、網路微分段及強化端點防護進行適當保護，同時將重要度分為Tier1 ~ 3三個等級，將不同Tier進行網路隔離、存取控制與持續監控，2022資安保護類投入NT$X,XXX,XXX
3. 偵測類: 為加速可疑事件判斷，導入NDR等APT偵測預防機制，快速找出異常行為並進行阻擋；2022資安偵測類投入NT$X,XXX,XXX
4. 回應類: 依事故回應計畫，針對可疑異常事件進行分析、判斷，確認事件為真則依影響範圍進行事故等級分類與處置，為強化機房實體安全與持續監控，故針對重要資產導入數位證據收集；2022資安回應類投入NT$XXX,XXX
5. 復原類: 為了強化企業資安韌性，使產品與服務交付不因黑天鵝或灰犀牛事故影，故強化資料保護最後一哩路，除了秉持備份3-2-1原則，同時導入AirGap降低資安事故的回復時間；2022資安恢復類投入NT$X,XXX,XXX

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 資安產品或服務分類 | | 說明 | 廠牌規格 | 取得日期 | 幣別 | 取得原價 |
| 辨識 | 資通安全治理及風險評估 | 聘請顧問導入資安框架與政策 | 顧問服務 |  | TWD |  |
| 辨識 | 資產管理 | 資產盤點 | 資產盤點系統 |  | TWD |  |
| 辨識 | 資通安全治理及風險評估 | 弱點掃描系統導入 | 弱點掃描軟體 |  | TWD |  |
| 保護 | 網路安全防護 | Server與Client網路分段 | Cisco Switch |  | TWD |  |
| 保護 | 網路安全防護 | Server與Client網路分段 | Cisco Switch |  | TWD |  |
| 保護 | 網路安全防護 | 次世代網路防火牆 | NGFW |  | TWD |  |
| 保護 | 網路安全防護 | 次世代網路防火牆 | NGFW |  | TWD |  |
| 保護 | 網路安全防護 | 資安風險改善 - 線路整改 | 機房整線工程 |  | TWD |  |
| 保護 | 端點裝置防護 | EDR端點防護 | EDR授權訂閱XXXU |  | TWD |  |
| 保護 | 網路安全防護 | 資安風險改善 - 機房實體安全 | 機房\_防火門 |  | TWD |  |
| 保護 | 網路安全防護 | 資安風險改善 - 機房實體安全 | 機房\_玻璃窗震動偵測 |  | TWD |  |
| 保護 | 網路安全防護 | 資安風險改善 - 機房實體安全 | 機房\_佈覽安全改善 |  | TWD |  |
| 偵測 | 端點及網路偵測與回應 | NDR導入 | AI+SOC Service |  | TWD |  |
| 回應 | 數位證據保存 | 數位證據收集與保存 | Storage+CCTV |  | TWD |  |
| 復原 | 異地備援 | 異地備援存儲請購 | Storage |  | TWD |  |
| 復原 | 資料備份 | AirGap備份解決方案導入 | Storage |  | TWD |  |
| 復原 | 資料備份 | AirGap備份解決方案導入 | 磁帶機 |  | TWD |  |
| 復原 | 資料備份 | AirGap備份解決方案導入 | 光碟櫃 |  | TWD |  |
| 復原 | 資料備份 | AirGap備份解決方案導入 | 10G Switch |  | TWD |  |
| 總計 |  |  |  |  | TWD | XX,XXX,XXX |

執行成效:

* 無重大資安事故
* 政策規範:增修XX份資安相關政策、程序書與管理辦法
* 防禦與聯防成效:每月阻擋約XXX萬餘次外部攻擊，對外服務均未受影響、成功偵測並阻擋XXX萬則廣告郵件及XX萬則威脅郵件、端點攔截威脅事件XX,XXX個
* 資安治理: 2022年成立專責資安部門，配置1位專職主管及2位專責人員，專責資安事件調查、威脅情報分析、漏洞管理以及資安新技術暨架構的評估和導入並完成X次資安管理會議
* 重大漏洞更新:定期更新X,XXX台設備防毒防護，成功率XX%；定期修補已知漏洞，完成X,XXX台裝置漏洞修補；主動通知X次重大安全性漏洞更新，更新完成率XX%，共修補系統及軟體漏洞XX,XXX個