數位發展部資通安全署
Administration for Cyber Security, moda

資安事件應變處理行動指引

115 年 7 月

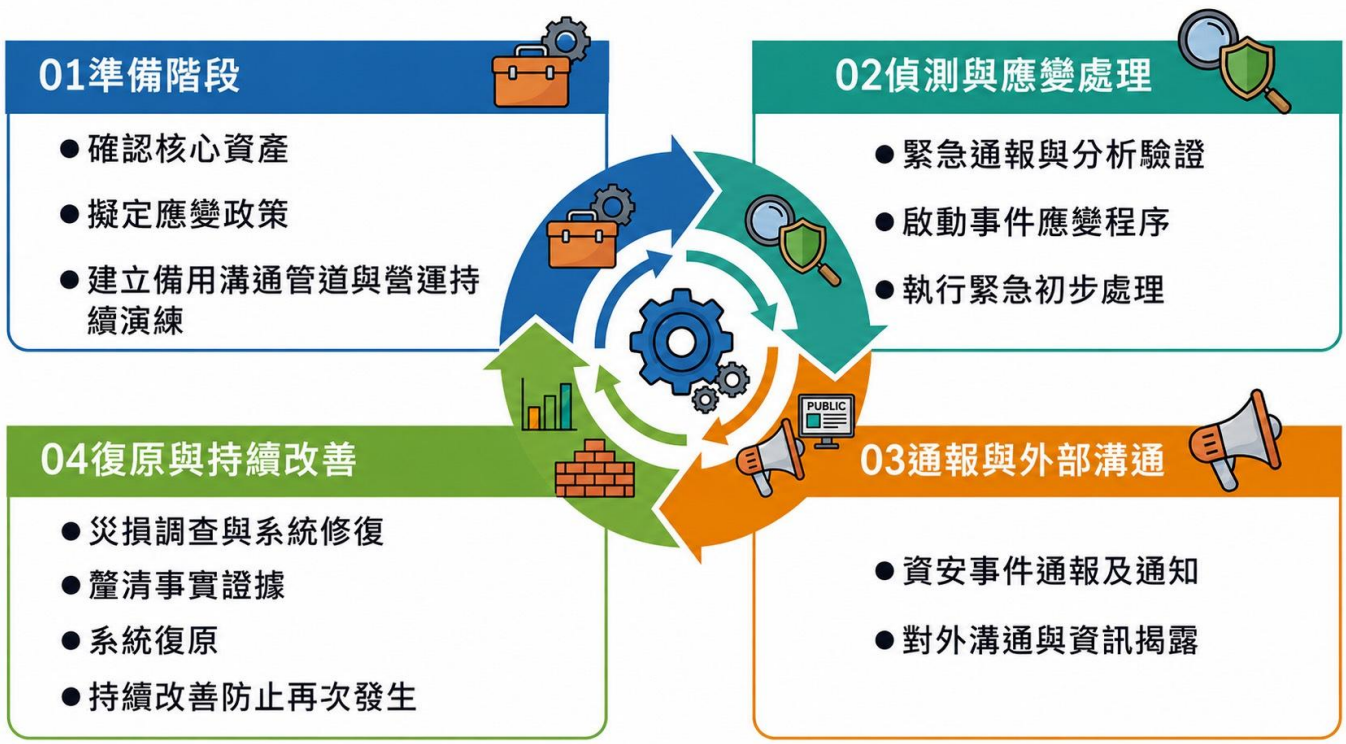
目錄

資安事件應變處理行動指引

面對日益複雜的資安威脅與風險，企業的營運韌性不僅取決於防禦強度，更強調「復原速度」與「韌性」。參照「中小企業基本資安防護指引」之帳號管理、設備和資料管理及資安意識培訓等三大面向，健全各項資安基本措施，固然能減少資安事件數量，但考量現實中並不存在「零風險」。尤其當防禦邊界被突破時，企業是否具備卓越的「資安事件應變處理能力」至關重要。

因此，本指引係延伸《中小企業基本資安防護指引》之內容，聚焦於資安事件發生後的應變與復原，將資安事件應變程序區分為「**準備階段**」、「**偵測與應變處理**」、「**通報與外部溝通**」、「**復原與持續改善**」等四大核心階段，並針對六大中小企業常見威脅情境，提供非技術人員按圖索驥的即時處理流程，協助企業在面臨資安危機的當下，能迅速採取適當措施降低損害與影響，即時應變並儘速恢復正常營運。

一、 資安應變四大核心階段



01 準備階段

確認核心資產

(一) 核心業務導向之資產盤點｜識別影響公司營運持續性之核心業務，並以此為基礎，縱向盤點與該業務流程相關之資訊/資料、軟體、硬體、網路及人力資源，建構完整的資產列表。

(二) 核心資產衝擊識別｜針對已盤點之資產，應進行機密性（Confidentiality）、完整性（Integrity）與可用性（Availability）等面向之營運衝擊分析（Business Impact Analysis, BIA），凡任一面向之潛在衝擊達到嚴重等級者，即定義為「核心資產」，並優先納入防護範疇。

擬定應變政策

(一) 建立事件通報及應變程序｜企業應預先編組「通報及應變小組」，明確賦予各應變角色（包含決策指揮者、技術處理人員、內外部聯絡人員）之權責，擬定應變機制應具備高度可操作性，並將執行步驟轉化為具體之標準作業程序（SOP），並輔以標準化檢核清單（參閱附件 1），協助應變小組在壓力環境下仍能按步驟執行、避免遺漏。

(二) 建立情境導向之資安事件應變處理機制｜因應資安威脅型態多元，建議針對意外災害等演練情境（如：風災、火災致使系統設備故障），以及高風險、高發生頻率之特定資安事件（如：勒索軟體、資料洩漏、DDoS 等）或其他複合式攻擊等，擬定應變處理機制，並定期辦理情境導向應變演練，以驗證事件通報、應變處置及復原程序之有效性。

建立備用溝通管道與營運持續演練

(一) 建置備用溝通管道｜為防止駭客攻擊導致公司內部的電子郵件或通訊軟體全面癱瘓，應預先準備好「獨立的備用通訊工具」（如：防竊聽的加密通訊軟體、或外部的應急通訊群組），確保在最嚴重的災難發生時，還是能互相聯絡、分配工作。

(二) 定期舉辦營運持續計畫演練｜每年至少舉辦一次「營運持續計畫演練」，並以公司可能遭遇情境（如：公司核心網路與外部中斷、電力供應異常、天然災害致使系統設備故障等）為模擬情境，藉此全面驗證管理階層之動態決策、跨部門資源調度量能，以及營運持續計畫之實效性。

02 偵測與應變處理

緊急通報與分析驗證

(一) 啟動內部緊急通報機制｜當人員偵測或發現系統異常特徵（如：未授權之異常登入、不尋常之檔案加密行為等），或確認發生資安事件時，應立即啟動內部通報程序，第一時間陳報公司管理階層，嚴格落實時效管理。（公司內部應變的建議時限請參閱附件 2）

(二) 外部情資蒐集關聯資訊紀錄｜若接獲外部利害關係人（如：客戶、合作夥伴、委外廠商）或國家級/產業別情資單位（如：TWCERT/CC、ISAC）之資安通報，應詳實收錄通報來源、觸發時間線、核心跡象及預估受影響範圍，並製作相關紀錄，作為後續數位鑑識與溯源之關鍵依據。

(三) 事件分析、驗證與分級｜如為非相關專業人員接獲資安通報時，建議記錄通報來源、知悉時間、事情經過、哪些系統受影響，即刻啟動外部專家應援或委外技術支援機制，包含立即執行事件驗證以排除誤報，透過交叉比對系統日誌分析（Log Analysis）、網路流量及端點行為，釐清攻擊範圍與入侵路徑等，並依據公司既定之損害評估標準，判斷事件嚴重性之分級。

啟動事件應變程序

(一) 啟動管理階層決策通報機制｜當公司判定資安事件影響到業務營運時，應立即啟動緊急通報程序，依公司既有通報程序通知管理階層，決定業務支援、資源調度或通知客戶等。

(二) 啟動通報及應變小組｜管理階層應依據事件對業務營運之衝擊程度，迅速啟動「通報及應變小組」，依循既定之應變政策，明確指派負責人與執行人員，適時納入外部專家應援或委外技術支援參與，確保各應變角色各司其職、高效協同。

執行緊急初步處理

(一) 實施事件圍堵與阻斷擴散｜評估受駭主機之外部連線狀態與潛在橫向移動風險，若存在擴散威脅，應立即啟動網路阻斷、隔離受影響設備或暫停受波及之系統服務，以控制損害範圍。

(二) 記錄應變過程並保全證據｜記錄資安事件應變處理歷程，優先執行記憶體與系統現況數據保全，嚴防相關儲存紀錄遭到抹除或覆寫，如：隨機存取記憶體中之揮發性數據、網路封包與關鍵攻擊日誌（Log）等，確保後續數位鑑識與證據之完整性，必要時協請外部專家應援或委外技術支援協助。

⚠重要提醒：在執行應變時，切勿隨意關閉電源或重啟系統。

03 通報與外部溝通

資安事件通報及通知

(一) 外部通報 |

- ✓ 通報資安事件：在發生資安事件時，可向台灣電腦網路危機處理暨協調中心（TWCERT/CC）進行線上通報。（網址：https://www.twcert.org.tw/tw/mp-1.html）
- ✓ 法規遵循：依據不同行業法規要求，通報各目的事業主管機關，如涉及個資洩漏時，亦同。
- ✓ 契約規定：執行受託業務，於知悉資安事件時，依契約要求通知委託機關，並採行補救措施。
- ✓ 涉及犯罪：向所在地警政機關報案。
- ✓ 發布重大訊息：上市櫃公司發生資安事件造成公司重大損害或影響者，應依規定發布重大訊息。

(二) 當事人通知 | 當企業重要資訊（例如個資、商業機密）被竊取、洩漏、或被竄改時，以電子郵件、簡訊或電話個別通知受影響之客戶、合作夥伴及監管機構；若受影響人數龐大導致逐一通知有困難，可改以官方網站公告、媒體發布等方式替代。

對外溝通與資訊揭露

(一) 擬定外部資訊揭露與公關危機處理策略 |

- ✓ 當事件衝擊造成難以逐一識別、或涉及社會公眾權益時，公司應啟動公關危機處理機制，並在第一時間指定對外發言窗口。
- ✓ 面對外界疑慮，應秉持正面、積極且誠懇的態度，主動說明公司目前積極辦理之清查進度、強化處理情形與資安防護措施，全程切忌隱瞞或卸責。
- ✓ 必要時透過官方管道或大眾媒體發布公開聲明，提醒客戶提高警覺；針對聲明內容、發布時機及目標受眾亦請審慎評估（資安事件公開聲明範本參閱附件 3），避免因資訊過度揭露導致二次資安威脅或公司商譽受損。

⚠ **重要提醒：資安事件期間，公司律定專人對外發言。**

(二) 資安事件進度報告與落實利害關係人追蹤 | 針對受影響之客戶、合作夥伴及監管機構，應主動提供事件處理進度、根本原因改善行動及追蹤報告。此外，應依據契約義務與相關法規，適時啟動損害評估、權益補償或法律賠償機制，以重建利害關係人信任。

04 復原與持續改善

災損調查與系統修復

(一) 現況盤點｜為做出正確的復原判斷，應以 5W1H（**When** 何時、**Where** 何地、**Who** 何人、**What** 發生何事、**Why** 為何發生、**How** 如何發生）之架構進行全面性現況調查，並即時彙整所有關聯之事件情資與鑑識軌跡。

(二) 執行修復｜依據事件情資進行根因追溯，並採取相對應之復原與強化措施，包含但不限於：安全性更新、重構系統配置、汰換或隔離受影響設備，以及執行受信任之資料還原，確保系統重啟後之安全性。

(三) 外部技術聯防與專家諮詢｜評估事件複雜度若逾越公司內部技術量能，應立即啟動外部協防機制，向資訊服務、資安或設備原廠、專業維運委外廠商或 TWCERT/CC 等外部專業機構尋求技術支援與鑑識。

(四) 動態進度回報管理階層｜於核心系統尚未復原之關鍵期間，資安負責人或資訊窗口應建立定期回報機制，針對事件處理進度、潛在營運衝擊及對業務持續性之影響範疇，適時回報管理階層提供決策支援。

釐清事實證據

保全足以證明事實關係的資訊與證據，並視需求進行數位鑑識調查，包括電腦硬碟、記憶體內資料、伺服器及網路設備的日誌紀錄（Logs）等。

系統復原

(一) 執行安全驗證與服務安全重啟｜經確認系統修復措施已落實、且通過漏洞修補與安全性合規驗證後，方得依序恢復先前暫停之系統、網路或業務服務，初期應持續監控系統維運情形，確保服務在安全無虞前提下穩健上線。

(二)提交事件結案報告與落實管理階層審查｜業務全面恢復常態化營運後，應彙整事件全貌、應變時序、損害評估、改善措施及後續精進對策，編製正式之「資安事件結案報告」，陳報管理階層進行審查，以落實資安持續改善機制。

持續改善防止再次發生

為避免資安事件再次發生，應進行根因分析，並研擬且落實根本性的防禦對策，包含導入新的技術防護措施、制定或修訂資安管理規範、強化員工資安意識教育訓練、優化公司應變體制與維運流程等。

二、 六大常見情境的關鍵應變行動

01 設備受感染異常

如何判斷是否遭遇設備異常感染？

惡意軟體感染之特徵識別

- **端點防護工具警示**

  優先查閱端點防護工具（如：防毒軟體、EDR）之威脅日誌，若防護系統發出惡意代碼檢出通知，應立即依據系統建議進行設備隔離。

- **效能與程序異常**

  設備運作效能顯著下降、系統無故頻繁重啟、執行中之應用程式異常終止，或背景自動觸發未知程序。

- **非預期之彈出視窗**

  系統頻繁彈出未知的廣告、錯誤提示，或假冒系統更新之詐騙視窗，要求授予高階管理權限。

- **帳號遭冒用發送異常訊息**

  同仁或外部聯絡人反應，收到由受影響設備帳號自動發出之推銷垃圾郵件、惡意連結或異常請款訊息。

該採取什麼行動？

當懷疑端點設備（個人電腦、筆記型電腦、行動裝置）疑似遭感染異常時，依據以下措施進行處理：

- **緊急應變處理**
  - **立即斷網隔離**

    拔除網路線、關閉 Wi-Fi 與藍牙，將可疑設備與公司網路隔離，防止惡意程式擴散。
    注意：應斷網、不要關機，強制關機會使記憶體中的數位跡證流失，影響後續調查。

  - **內部通報**

    立即通知公司資安負責人或資訊窗口。

  - **執行完整掃描**

    立即執行防毒軟體進行全盤掃描，並允許防毒軟體清除發現的所有威脅 。

  - **設備恢復出廠設定**

    資通訊設備及儲存媒體如發現連線惡意中繼站紀錄或存在惡意程式情形，應完成留存證據、保留日誌與惡意檔案採樣等程序後，還原至出廠設定；另外考量行動裝置的防毒軟體權限有限，如果遇到無法清除的惡意程式，最佳解決方式是留存資料備份後恢復出廠設定。

- **尋求專家協助**

  若上述方法無法修復，應積極尋求委外系統商、資安廠商或 TWCERT/CC 提供的資安諮詢協助 。

➢ **修復後強化**

系統完成威脅根除後，必須落實以下資安防護措施：

- **漏洞與修補管理**

  嚴格遵循原廠規範，立即將作業系統及應用程式更新至最新版本。

- **導入端點防護工具**

  安裝合規之端點防護工具並確認病毒碼更新至最新版，強制啟動「自動安全性更新」與即時排程掃描。

- **資料資產保全**

  定期執行全面性資料備份，同步檢查並確認設備已啟用加密機制，確保資料資產與數據安全。

不該採取什麼行動

➢ **未經評估便關閉所有關聯設備**

盲目對所有關聯伺服器或主機執行強制關機，可能導致核心業務中斷並造成巨大的經濟損失，在擴散風險受控的前提下，應採取「提升監控層級，維持系統有限度維運」之策略，待擬定妥善之營運持續應變計畫後再行移轉處理。

➢ **直接手動關閉可疑程序或逕行刪除異常檔案**

發現受駭時，若直接手動刪除惡意檔案或終止程序，將會徹底摧毀儲存於系統日誌與記憶體中的「數位跡證」，正確做法應交由資安技術人員優先進行惡意檔案採樣與現況保留，完成備份鑑識軌跡後，方可執行隔離與清除，以利後續的攻擊溯源與防禦優化。

02 帳號被盜

如何判斷帳號是否被盜？

當公司同仁發現帳號無法登入、或出現非授權之異常活動徵狀時，應視為資安事件，並立即依序採取以下緊急控制與防護措施。

該採取什麼行動

➢ 啟動帳號復原機制

立即尋求該平台服務供應商之官方技術支援及申訴，依循其帳號復原流程重新提交身分驗證證明，立即重新取得帳號之實質控制權。

➢ 清查電子郵件過濾與轉寄規則

立即檢視電子郵件之「過濾器」與「自動轉寄規則」，駭客常於後台暗中設定轉寄，藉此同步攔截驗證碼以實施二次入侵，如查獲異常規則，應即刻刪除。

➢ 強制執行密碼變更

■ 即刻變更密碼

於權限恢復後，立即重新設定該帳號之長、複雜且難以破解的密碼（密碼長度至少 15 碼），並評估使用密碼管理工具。

■ 阻斷駭客密碼盲測

若有其他平台「重複使用」相同密碼，必須同步全面執行變更，嚴防駭客利用此受駭帳號之密碼，對其他業務系統進行試探，進而造成其他平台帳號受駭。

➢ 將使用帳號之所有裝置和應用程式中登出

完成密碼變更後，務必進入帳號安全設定，執行「強制登出所有裝置與應用程式」，徹底切斷其非授權之存取管道。

➢ 採取二階段驗證（2FA）

針對所有核心帳號或雲端服務，全面強制啟用二階段驗證，透過動態領取一次性驗證碼（如：生物辨識、使用手機 App 取得代碼、簡訊驗證碼等）強化帳號安全，確保即便密碼不慎洩漏，駭客仍因缺乏其他因子而無法入侵。

➢ 更新應用程式和裝置

確保維持所有端點設備（作業系統、瀏覽器、應用程式及資通訊設備）處於最新版本狀態，並開啟「自動安全性更新」，透過安全性更新封鎖已知漏洞，降低駭客透過惡意軟體側錄密碼風險。

➢ 發布利害關係人防詐預警

主動通知與該帳號業務往來之聯絡人、內部同仁、客戶或社群追蹤者，表明帳號曾遭短暫篡改，提醒利害關係人對近期以該帳號名義發出之請款簡訊、惡意連結或異常檔案保持高度警惕，防止威脅向外橫向擴散。

➢ 審查帳號關聯來往

帳號受駭常衍生外圍系統連帶淪陷，針對受害帳號應全面清查綁定該帳號之網路銀行、第三方支付、企業採購系統等，防範未授權之異常採購與實質財務損害。

不該採取什麼行動

➢ 保持現狀並持續使用受駭帳號

當帳號出現異常徵狀時，切勿抱持「再觀察」之消極態度繼續使用，駭客通常已於系統後台建置惡意後門或重設存取憑證，意圖持續性潛伏與奪取帳號使用權限，若未即刻中斷連線並重置帳號，將使駭客得以在免受偵測的狀況下，持續竊取公司敏感資料或擴大橫向滲透範圍。

03 網路釣魚

如何判斷是否遭遇網路釣魚？

凡收到來源不明、急迫催促、或要求驗證帳號之可疑訊息，秉持「不點擊未知連結、不下載不明附件、不輸入敏感資訊」之原則，若不慎觸發或洩漏資訊，立即採取以下緊急應對措施。

該採取什麼行動

➢ 涉及公司或個人敏感資訊或憑證

■ 金融帳戶或卡號洩漏

立即聯絡發卡銀行或金融機構進行掛失控管，若該帳戶具備網路銀行功能，應即刻透過 App 或網銀執行「線上鎖卡」或暫停交易功能。

■ 帳號被盜

若發現帳號無法登入、密碼遭篡改或有異常登入活動，立即啟動平台的帳號申訴與復原機制，**並參閱「02 帳號被盜」專章**。

■ 設備疑似受駭或遭惡意植入

應立即啟動設備裝載之端點防護工具（如：EDR、防毒軟體）執行掃描，並依據端點防護工具建議進行惡意程式隔離與清除，若設備已受嚴重感染，**參閱「01 設備受感染異常」專章**。

■ 身分憑證與密碼洩漏

若洩漏之密碼具「跨平台重複使用」之情形，應立即變更所有關聯帳號之密碼，並強制啟用二階段驗證（2FA）以強化帳號安全。

■ 金融帳戶已遭受實質財務損失

第一時間通知銀行啟動攔阻匯款，同步撥打「165 反詐騙諮詢專線」，並備妥相關對話紀錄與交易憑證，前往所在地警政機關報案處理。

■ 公務設備（電腦/行動裝置）觸發異常訊息

應立即通報公司內部資訊/資安人員，或啟動外部專家應援或委外技術支援機制，以利進行事件評估、端點隔離與後續資安事件應變處理。

➢ 誤觸可疑連結之緊急處理程序

當不慎點擊可疑連結、簡訊或電子郵件附加網址時，依據實際觸發行為採取相對應之應變作為：

情況一：僅點擊連結，未進行後續操作（潛在風險控制）

■ 風險評估

若僅點擊連結，但未輸入任何個人資訊、未下載任何檔案、且未同意安裝任何軟體，實質受駭風險相對較低。

■ **防禦作為**

應保持警惕並加強監控，於後續數日內密切留意該裝置之帳號登入通知、非預期之驗證碼簡訊及電子郵件異常活動。

情況二：已觸發執行或洩漏敏感資訊（實質損害控制）

■ **不慎下載檔案或依指示安裝未知軟體**

應立即啟動設備裝載之端點防護工具（如：EDR、防毒軟體）執行掃描，並授權防護軟體進行惡意程式隔離與全面清除，若設備已出現嚴重受感染表徵，立即斷網**並參閱「01 設備受感染異常」專章**。

■ **已洩漏帳密資訊**

若洩漏之密碼具「跨平台重複使用」之情形，應立即變更所有關聯帳號之密碼，並強制啟用二階段驗證（2FA），以中斷駭客持續存取其他帳號平台。

■ **已洩漏金融帳戶或信用卡資訊**

應即刻聯絡發卡銀行或所屬金融機構申請帳戶掛失，若該帳戶支援行動銀行/網路銀行，應第一時間透過官方 App 執行「線上鎖卡」或暫停交易功能，以防堵衍生之財務損失。

➢ **收到可疑訊息或發現可疑網站**

■ **啟動「165 全民防騙網」情資舉報**

立即前往內政部警政署「165 全民防騙網」官方平台，執行「我要檢舉」程序，詳實上傳涉嫌詐騙之對話軌跡截圖與惡意 URL 連結，提供執法機關進行犯罪溯源與情資比對。

「165 全民防騙網」https://165.npa.gov.tw

■ **導入《網路詐騙通報查詢網》跨域阻斷機制**

將發現之可疑網址提交至數位發展部「網路詐騙通報查詢網」，透過該平台與主流社群及通訊巨頭（如 Meta/FB、Google、LINE 等）之自動化聯防連動機制，如經審查屬實，即刻要求第三方平台採取預防性下架與跨域阻絕措施。

「網路詐騙通報查詢網」https://fraudbuster.digiat.org.tw

不該採取什麼行動

➢ **勿繼續使用已洩漏之密碼**

若密碼有跨平台重複使用，應立即變更所有關聯帳號密碼並啟用二階段驗證（2FA）

➢ **勿隱瞞設備的異常狀況**

當帳號出現異常徵狀時，切勿抱持「再觀察」之消極態度繼續使用，駭客通常已於系統後台建置惡意後門或重設存取憑證，意圖持續性潛伏與奪取帳號使用權限，若未即刻中斷連線並重置帳號，將使駭客得以在免受偵測的狀況下，持續竊取公司敏感資料或擴大橫向滲透範圍。

04 商業支付詐欺

如何知道自己是否是受害者？

駭客常採用「社交工程攻擊」，透過假冒合作廠商、外部律師或內部高階經理人等，針對企業員工或高階主管發送高度偽冒之電子郵件，引導同仁誤信其為合法聯絡人。

常見詐騙態樣：

- **隨信附帶看似合法的惡意發票或請款單據，誘使下載並觸發惡意程式（如木馬、勒索軟體）。**
- **以「機密商務變更」、「審計查核」或「緊急契約」為由，要求將商務款項匯入非約定之銀行帳戶**

該採取什麼行動？

如果認為自己被騙進行欺詐性付款，請保持冷靜，並採取以下步驟：

- **第一時間進行資安通報**

  應立即向公司內部資訊/資安人員以及管理階層進行報告，資安團隊、外部專家應援或委外技術支援越早介入，越能即時阻斷駭客對系統的持續潛伏，並協助追蹤營運衝擊。

- **保存核心跡證與法務諮詢**

  完整留存該詐騙郵件之標頭、通訊紀錄、惡意附件及匯款憑證等原始跡證，切勿刪除，同步諮詢公司法務人員，以利後續法律追訴與保險理賠。

- **啟動金融止血與圈存機制**

  立即透過金融機構官方管道（官方網站或經確認之專線電話）直接聯絡往來銀行，通報遭遇詐騙，並要求全面凍結該筆異常交易或啟動攔阻匯款。

不該採取什麼行動？

為維護公司財務安全，在面臨異常付款要求時，嚴禁執行以下行為

- **未依程序執行匯款**

  合法的商業合作夥伴皆理解並尊重企業的財務覆核與內部控制程序，凡以「時間緊迫」、「極度機密」為由，對公司依照正常流程辦事而展現過度憤怒、焦慮或施加壓力者，皆具備高度詐騙特徵。

- **未經驗證執行匯款**

  面臨任何變更匯款帳戶或緊急請款之要求，必須向對方窗口進行二次驗證（如撥打原契約登記之市話、傳真或面對面親自確認），絕不可直接回覆該封可疑郵件。

  ⚠ **重要提醒：未經驗證切勿支付或口頭承諾付款。**

05 勒索軟體攻擊

該如何判斷是否為勒索軟體攻擊？

- **資料全面遭鎖定**

  系統內之核心數據、檔案或資料庫副檔名遭異常篡改，導致無法正常讀取或存取。

- **具備勒索告示**

  系統桌面或目錄內自動生成文字檔或網頁，內容通常包含匿名聯繫之電子郵件、匿名網址，並要求以加密貨幣（如 BTC、XMR）支付贖金以獲取解密金鑰。

- **雙重勒索手法**

  攻擊者通常宣稱已預先竊取公司敏感數據，並威脅若未於時限內交付贖金，將於暗網公開揭露或販售。

該採取什麼行動

當確認遭遇勒索軟體攻擊時，應在「不關機」的前提下，立即依序啟動以下遏制措施，以防損害擴大：

- **緊急控制與遏制**
  - **立即中斷端點連線**

    迅速拔除受影響設備（桌機、筆記型電腦、伺服器）之有線網路線，同步關閉 Wi-Fi 或行動網路（4G/5G）連線，杜絕橫向移動。

  - **核心網段阻斷**

    若評估事件呈大規模擴散趨勢，應立即通報公司內部資訊/資安人員，或由資安團隊、外部專家應援或委外技術支援介入，視情況停用相關 VLAN、隔離受影響網段，或中斷對外網際網路連線，以防止勒索軟體持續橫向擴散、加密雲端同步資料，或與指揮控制（C2）伺服器通訊，降低事件影響範圍。

- **特權帳號憑證控管**
  - **即刻重置特權帳號密碼**

    立即強制重置疑似遭入侵或可能受影響之網域管理員（Domain Admin）及公司核心特權帳號之密碼，中斷駭客已掌握的控管權限。

  - **預留應變通道：**

    在執行帳號停用、權限限縮或存取控制措施時，必須確保內部應變團隊保留具備實體主控台（Console）存取權限之緊急應變帳號（Break-glass Account），避免在系統復原期間因權限鎖定導致技術團隊遭到阻絕。

- **執行乾淨重構與安全部署**
  - **硬碟格式化與作業系統重灌**

    針對受影響設備執行硬碟低階清除，並從受信任之合法來源重新安裝作業系統。

- **部署乾淨網路與安全性更新**

  將受影響設備完全隔離，立即下載並套用安全性更新，封鎖漏洞。

- **端點防護全面監控**

  安裝、升級並啟動設備部署之端點防護工具，如：端點偵測與回應（Endpoint Detection and Response, EDR）、防毒軟體等工具執行掃描，建構即時主動防禦量能。

➢ **備份還原之資安審查**

- **備份檔惡意程式清查**

  在執行任何資料還原前，必須對備份鏡像檔進行獨立之惡意程式與源碼掃描，嚴防還原檔案中夾帶潛伏之勒索軟體主程式或駭客預留之腳本。

- **常態化復原**

  確認備份檔案安全無虞後，方可將資料導入已完成清理與重構系統環境。

➢ **持續性維運監控**

完成重啟並重新接入營運網路後，公司內部資訊/資安人員或資安團隊、外部專家應援或委外技術支援應針對內網流量進行深度封包分析（Deep Packet Inspection, DPI），並持續執行端點掃描，嚴密監控是否有非預期之異常連線、殘留惡意程式或攻擊者再次入侵之特徵。

不該採取什麼行動

➢ **執行強制關機或系統重啟**

許多勒索軟體在將檔案加密後，其所使用的「加密金鑰或相關執行資訊」可能仍短暫儲存於設備的隨機存取記憶體（RAM）當中，若同仁未完成必要之證據保留，在此時執行關機、拔除電源或重新開機，將會瞬間遺失記憶體內的所有「揮發性證據（Volatile Evidence）」。這不僅會徹底摧毀後續資安專家利用數位鑑識擷取加密金鑰，**於無須支付贖金的情況下完成資料解密，取得解密資訊或其他重要證據之可能性**，也將增加數位鑑識與攻擊足跡溯源的難度。

06 阻斷服務攻擊（DoS/DDoS）

該如何判斷是否為阻斷服務攻擊（DoS/DDoS）？

於遭遇阻斷服務攻擊（DoS/DDoS）期間，公司之目標網站、核心網路或雲端服務架構將因資源耗盡，導致系統異常、連線不穩定，甚至引發服務中斷，致合法外部用戶與內部使用者無法正常存取。

凡此類攻擊波及關鍵業務功能時，將對公司之營運生產力造成直接性重創。實質衝擊包含但不限於：線上交易中斷所致之即時銷售與訂單損失、內部營運流程停擺等。

該採取什麼行動

- **流量與類型分析**

  迅速聯絡網路服務提供商（Internet Service Provider, ISP）或主機代管業者，協助分析並確認攻擊流量的類型（如 UDP Flood、HTTP GET Flood）。

- **啟動業務持續營運計畫**

  若核心系統因攻擊服務中斷，應立即切換至替代的人工作業、紙本替代方案或備用系統，維持最低限度之業務運作，並同步計算中斷損失 。

- **尋求電信服務商/流量清洗中心支援**

  聯繫電信服務商或主機代管商，評估能否透過基礎防護或啟用備援 IP，或導入內容傳遞網路（Content Delivery Network, CDN）與流量清洗服務（Traffic Scrubbing Service），將惡意流量導流過濾。

不該採取什麼行動

- **直接關閉伺服器或強制關機**

  盲目對伺服器或主機執行強制關機，可能導致核心業務中斷並造成巨大的經濟損失，且會使記憶體中的數據與日誌（Logs）跡證流失。

- **單純被動等待流量自行消退**

  遭遇攻擊導致服務異常或中斷時，應主動聯絡 ISP/主機代管業者分析流量類型、啟動業務持續營運計畫（如替代方案），並聯繫電信商/流量清洗中心導入流量清洗服務。

三、 給公司經營決策階層的核心思維

01 資安治理須由管理階層負責

資安不再只是 IT 部門的責任，而是經營管理階層的「商業經營與治理責任」，當事件發生時，受損的不僅是企業信用、品牌商譽，更可能面臨巨額行政罰鍰，經營管理階層應持續評估提供足夠資源，建立企業資安韌性及持續營運能力 。

02 資安事件應變計畫須由管理階層審查與核可

由 IT 或資安部門撰寫資安事件應變計畫，若無經營管理階層審查與正式核可，事發時往往會因為跨部門調度失靈（如公關、法務與 IT 互相踢皮球）而形同廢紙 。

03 依法通報與妥善對外溝通

在現代嚴格的監管法規環境下，隱匿不報往往會招致更嚴厲的行政處罰與商譽影響，遵循通報時效並保持透明度，才是合法合規且保全企業資產的最佳路徑。

附件 1、資安事件應變處理檢核清單

項次	資安事件應變檢核清單	完成	
		是	否
一	**準備階段**		
1.1	完成資產盤點	☐	☐
1.2	識別核心資產	☐	☐
1.3	預先編組「通報及應變小組」	☐	☐
1.4	建立情境導向之資安事件應變機制	☐	☐
1.5	建置備用溝通管道	☐	☐
1.6	定期舉辦營運持續計畫演練	☐	☐
二	**偵測與應變處理**		
2.1	啟動內部緊急通報機制	☐	☐
2.2	依據資安事件損害評估判斷事件分級	☐	☐
2.3	通報管理階層決定業務支援、資源調度或通知客戶	☐	☐
2.4	啟動「通報及應變小組」	☐	☐
2.5	啟動網路阻斷、隔離設備或暫停系統服務	☐	☐
2.6	記錄應變過程並保全證據	☐	☐
三	**通報與外部溝通**		
3.1	資安事件通報	☐	☐
3.2	通知受影響客戶、合作夥伴及監管機構	☐	☐
3.3	指定對外發言窗口並適時揭露資訊	☐	☐
3.4	針對利害關係人主動提供資安事件進度報告與落實追蹤	☐	☐
四	**復原與持續改善**		
4.1	針對災損情形執行全面性現況調查	☐	☐

項次	資安事件應變檢核清單	完成	
		是	否
4.2	執行修復，包含安全性更新、重構系統配置、汰換或隔離設備等	☐	☐
4.3	尋求外部技術支援與專家諮詢	☐	☐
4.4	動態進度回報管理階層	☐	☐
4.5	確認完成修復後，依序恢復暫停之系統、網路或業務服務	☐	☐
4.6	提交資安事件結案報告	☐	☐
4.7	持續改善防止再次發生	☐	☐

附件 2、資安事件應變里程碑建議時限

公司內部應變的建議時限，屬自訂管理目標，非法規強制，各公司可依業務衝擊分析（BIA）調整。

資安事件應變里程碑	建議時限	說明
發現異常 → 內部初步通報（資安 / 資訊窗口）	15 分鐘內	確認或高度懷疑事件即通報，不待查明全貌
陳報管理階層	1 小時內	影響營運或涉個資 / 金流者，口頭或訊息先報
啟動通報及應變小組	1 小時內	由管理階層依衝擊程度啟動並指派角色
開始記錄與證據保全	立即、與應變同步	記錄時間軸，保全揮發性資料，勿關機重開
圍堵 / 隔離受害設備	確認擴散風險後立即	拔網路線、隔離設備，暫停受波及服務
（涉金流）請銀行圈存 + 撥 165	把握 30 分鐘黃金時間	成功率隨時間快速下降，越快越好

附件 3、資安事件公開聲明範本

聲明發布日期：YYYY 年 MM 月 DD 日（必要時可註記「第 X 版」或「補充說明日期」）

親愛的客戶 / 合作夥伴 您好：

針對近期本公司遭遇之資安事件，本公司深感抱歉並極為重視。我們秉持透明、負責之原則，在此向全體利害關係人說明事件經過、調查結果、已採取的應變處理，以及後續改善措施。

一、 事件說明與影響範圍調查

本公司於 YYYY 年 MM 月 DD 日（發現時間）偵測到內部【系統/伺服器名稱，例如：CRM 系統 / 檔案伺服器】出現異常存取行為。我們第一時間即啟動內部資安事件應變機制，並會同鑑識團隊【資安公司/ 第三方專業資安鑑識機構】開展全面調查。

現階段釐清狀況如下：

1. **系統服務情形**：本公司【核心服務 App / 交易系統 / 支付資料庫】未受影響，仍維持對外服務，另針對【系統敏感資訊，例如：信用卡號、銀行帳號、登入密碼、交易密碼等】均受獨立加密機制保護，確認安全無虞。
2. **受影響資料範圍**：經查本次事件涉及部分【例如：內部員工作業檔案 / 歷史專案會員資料】。
    - **可能受影響之欄位**：包含【姓名、電話號碼、電子信箱、通訊地址】等。（非每筆資料均包含所有欄位，預估受影響筆數約為 XXXX 筆）
    - **未受影響之欄位**：身分證字號、財務與支付資訊、密碼等敏感資料均不在受影響範圍內。

二、 應變處理與因應措施

事件發生後，本公司已迅速採取以下應變程序與緊急初步處理：

1. **系統阻斷與隔離**：第一時間切斷受影響系統之外部連線及異常存取管道，防止損害與威脅進一步擴散。
2. **依法通報與警政報案**：已依相關法令規定，於時限內向主管機關【例如： 產業目的事業主管機關】進行資安事件通報，並向警政署刑事警察局/所在地警察機關正式報案處理。
3. **暫停金融帳戶交易功能**：已聯絡金融機構申請「線上鎖卡」及暫停交易功能，並要求全面凍結異常交易，攔阻匯款。
4. **引進外部專家：** 已委請第三方資安鑑識專家協助進行全面的技術調查與系統復原作業。

三、安全建議與提醒

為確保您的資訊與資產安全，本公司特別提醒您留意以下事項：

1. **警惕可疑訊息**：請留意近期可疑的來電、簡訊、電子郵件或社群訊息，切勿點擊不明連結、下載未知附件，或提供個人敏感資訊。

2. **嚴防詐騙冒用**：本公司絕不會以電話、簡訊或電子郵件要求您提供銀行帳號、信用卡資訊、驗證碼，或引導您操作 ATM / 網路銀行進行匯款或解約。
3. **帳號安全自主管理**：若您在其他平台使用了相同之密碼，建議您立即變更密碼並開啟二階段驗證（2FA），以確保帳號安全。

四、 承諾與持續改善

本公司承諾全面升級資安基礎建設與防護機制，為確保未來不再發生類似事件，將持續投入以下資源:

1. **技術與系統升級：**全面升級系統資安防護，並導入 XXXX 機制/系統【例如：零信任、2FA 等】，以最高標準強化基礎建設，確保系統安全。
2. **內部管理與訓練：**全面檢討內部管理機制，嚴格落實資料存取的最小權限原則，並大幅強化全體員工的資安教育訓練。
3. **漏洞修補與防護：**已將作業系統及應用程式更新至最新版本、受感染設備恢復出廠設定，並從受信任之合法來源重新安裝作業系統。
4. **端點防護：**安裝合規之端點防護工具，強制啟動「自動安全性更新」與即時排程掃描，並確認病毒碼已更新至最新版。

五、 專責聯繫窗口

如您對本次資安事件有任何疑慮、查詢需求或發現異常狀況，歡迎透過以下官方管道與我們聯繫，我們將有專人為您服務：

- **客服專線**：（02）XXXX-XXXX（服務時間：週一至週日 09:00–18:00）
- **客服信箱**：service@yourcompany.com.tw
- **官方網站說明專區**：https://www.yourcompany.com.tw/security-notice

最後，對於本次事件造成的疑慮、不安與不便，我們再次致上最深切的歉意，本公司將持續投入必要資源強化資安防禦韌性，嚴格保護用戶的個資，並加強監控及落實資安防護管理。

【企業名稱/機構名稱】敬上