資料來源：資訊安全網

處理資訊保安事故須知

近年，全球不斷發生不同類型的資訊保安事故，例如遭到黑客攻擊、入侵或勒索，香港亦屢見不鮮。面對黑客肆虐及資訊保安事故時，各行各業都應該採取一些基本措施。為此，資訊安全網為企業提供有關資訊保安事故的簡介、應變措施及注意事項等訊息，有助企業加強網絡保安，防患於未然。

去年，全球多個地方遭受到 WannaCry 勒索病毒的影響，為降低被惡意攻擊的風險，企業應制定一系列的防範及應變措施，以加強資訊保安的防衛。

何謂資訊保安事故

資訊保安事故是指在資訊系統及／或網絡上的負面事情，對資訊的機密性、完整性、可用性、不可否認性和認證等方面構成威脅。以下是負面事情的一些例子：

- 盜竊及爆竊
- 天然災害，例如水災、颱風、暴雨
- 來自周遭環境的潛在危險
- 數據線路故障
- 系統當機
- 小包氾濫
- 未經授權接達或使用電腦系統的資源
- 未經授權使用他人帳戶
- 未經授權使用系統權限
- 網頁竄改
- 闖入／入侵系統
- 大規模電腦病毒攻擊

然而，天然災害、硬件／軟件失靈、數據線故障、電力中斷等事故，並非以資訊保安事件處理，而是以系統維修及災害應變措施看待。

何謂資訊保安事故處理？

資訊保安事故處理是指一套連貫的程序，管理在保安事故發生前、發生時和發生後所執行的活動。

保安事故處理始於規劃、準備資料及制定適當程序（例如升級處理和保安事故應變程序），以備日後遵照執行。一旦偵測到保安事故，負責保安事故應變的各方須按照預定程序實施應變。保安事故過後，應採取跟進行動評估事故，並加強保安保護措施，以防止事故再度發生。

UPM Finesse Classic Matt, 90 gsm

保安事故應變的目標

- 將商業損失和隨之而來的責任減至最低；
- 將可能發生的衝擊，例如資料外泄、資料受損和系統受襲等機會減至最低；
- 確保回應是有系統性和有效率的，並且可以迅速復原受影響的系統；
- 確保所需的資源，包括人手、技術等都齊備；
- 確定負責的人士清楚知道他們的職責，並遵從事先訂制的步驟處理事故；
- 確保應變的行動被認可和互相協調；
- 防止類似的襲擊和破壞再次發生；以及
- 處理和法律有關的事項。

不論風險緩減措施如何優秀，將保安事故的衝擊度和發生機率減至最低，但事故還是會出其不意地襲擊，所以企業必須作好準備。

保安事故應變的法律和合約考慮

有些保安事故與罪行有關，例如竄改別人網頁、破壞伺服器、發放垃圾電郵和盜取資料在香港都是違法的。然而，掃描連接埠便不屬於刑事罪行，因此企業必須要留意不同國家有關網上罪行的法例是不同的。如果事故涉及違法活動，企業應該向執法機關報告，如有任何問題，亦可以向執法機關查詢。

起訴入侵者的兩難

若果企業想起訴入侵者，必須考慮以下幾個問題：

- 企業是否應保持連接網絡，以便追蹤入侵者的活動？
- 以上的舉動會否讓入侵者繼續襲擊企業的系統，造成更大的傷害？
- 在恢復業務和追蹤和起訴入侵者之間，企業應如何抉擇？

不論所選的答案是什麼，企業都應該：

- 讓管理層做決定；
- 根據事先制定的優先次序和條件，實施事故回應行動；
- 確認決策過程的結構和通知執法機關。

搜集證據時的考慮

事故應變小組（又稱 IRT）人員會接觸第一手證據，例如日誌檔案和系統狀態資料（例如系統時間，正在運作的過程和連接的電腦），但最重要的是小組人員知道如何處理這些證據。以下是處理證據的一些指引：

- 一件證據是一個事件或事實。
- 電子證據一定要儘快搜集。
- 保持證據的先後次序。一連串的證物是一段歷史，可以在法庭上展示證據如何搜集、分析、運送和保存的時序，而一連串清晰的證物能表示它們是可信的。
- 收集證據時要根據一定的步驟，並使用適當的（沒有受污染）工具。
- 證據要受到保護，不可以讓未經授權的人接觸證據，和不可以讓證據被更改或破壞。要得到授權和有第三者在場才可以運送或複印證據。

事故應變小組人員應該記錄行動和結果，並應該應用收集證據的指引：

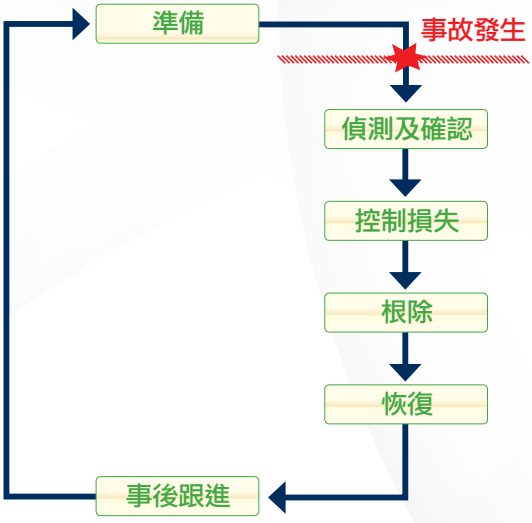
- 清楚及整齊地依時序記錄事件，並標示當時的時間。可以的話，用預先印製的表格去統一記錄的格式，有需要時可使用錄音和錄像。
- 寫下事實，而非猜想或不肯定的推測，不清楚和不小心的說話可能會削弱證據的說服力。
- 發現錯誤後要立刻改正，並記錄錯誤的原因。

追蹤入侵者來源的考慮

惡意的入侵可能使技術人員產生強烈的反應，但不可以衝動地即時追捕入侵者而忽略減低保安的衝擊。以下是有關追蹤入侵者來源的建議：

- 不要考慮「反擊」這策略。因為發動襲擊的一方可能也是被入侵的受害者；其次，欺詐技術會令人錯誤推測襲擊的來源，而且根本沒有法理基礎進行報復。
- 保持低調。小心技術人員的行為會令入侵者知道自己已被發現，並因此刪除其足跡或破壞整個系統。
- 技術人員要熟悉技術性步驟和工具，確保追蹤過程有效率和不被發現。

保安事故應變的六步曲



保安事故應變共分為六個步驟，而成功的關鍵就是要有充足的準備。提早作出恰當的計劃，可以確保回應行動為人所知、互相協調和有系統地進行，這亦幫助管理層在追查保安事故和降低破壞程度時作出恰當而有效的決策。這計劃包括加強保安防護、適當地對事故作出回應、復原系統和其他跟進行動。

準備

保安事故應變計劃能夠提供從上而下的事故應變管理模式，保證回應的質素和時間。

- 決定內部政策。
- 確保事故應變策略和公司的保安政策相容，事故應變小組有足夠的權力進行保安行動，例如在重要時刻關閉公司的伺服器。
- 界定事故應變小組和參與保安事故處理過程的人的角色和責任。
- 界定其他職員的角色和責任，並將決定通知管理人員。
- 建立一個列表，顯示資訊資產和服務的優先次序和可以接受的關閉時間。
- 建立匯報機制、升級處理程序和保安事故應變程序。這些程序都應該通知每一個職員，包括人事、管理部門，讓他們參與和遵守。
- 建立預警系統，例如維持一個足夠應付日常工作需要的簡單技術環境和容易使用的服務台。
- 建立和維護良好的備份策略。
- 建立和維護良好的緊急事故聯絡電話表。
- 從香港電腦保安事故協調中心 (HKCERT) 和其他電腦危機處理中心 (CERT 中心) 更新指引、檢核表和工具。
- 透過培訓和分享建立事故應變小組的知識和技術。
- 提供足夠的培訓，確保職員懂得處理緊急保安事故。
- 教育用戶緊急應變步驟和報告事故的方法。
- 將電腦系統的時鐘同步。
- 建立一個電腦系統監控和警報機制，例如安裝入侵偵測、抗電腦病毒和內容過濾工具，開啟系統及網絡審計記錄功能，定期利用保安掃描工具進行保安檢查。

偵測及確認

- 監控不正常事件，例如錯誤訊息、日誌記錄中的可疑事件、不正常的效能表現和容量不尋常地增加。
- 決定問題的種類和衝擊的程度。
- 用標準事故記錄表格作記錄。
- 參考搜集證據指引處理資料。
- 證實確有其事後，馬上把受影響的系統全面備份，並存放在一個安全的地方。
- 保留事故的記錄，例如審計日誌、帳戶日誌等等。
- 通知在緊急事故聯絡電話表上的高層管理人員和其他有關人士（包括事故應變小組(IRT)、互聯網服務供應商、網絡服務供應商）及通知系統擁有者。執行「有需要才知道」政策，需要時使用另外的安全通訊頻道。

制止情況惡化

這階段的行動包括：

- 評估因事故對系統內的數據和資料衝擊程度，確定有關資料是否已經被破壞或感染；
- 保護敏感或重要的資料和系統，例如將重要資料轉移到其他和受影響系統或網絡完全分隔的媒體（或其他系統）；
- 決定受影響系統的作業狀態；
- 製作受影響系統的映像，作為以後跟進行動的證據；
- 記錄在這階段進行過的一切行動；以及
- 檢查所有透過分享網絡服務或其他信任連繫和受影響系統有連繫的系統。

這階段其中一個重要的決策是繼續還是停止受影響系統的運作。這大多是根據事故的嚴重性、系統的要求、對公司形象的影響及預設的目標和事故處理計劃的優先次序。所需要採取的行動包括：

- 暫時關閉或分隔受影響的主機或系統，避免對其他相連的系統產生傷害。這在可能傳播得特別快的事故、載有敏感資料的電腦或防止受影響系統被人利用進行其他襲擊等情況下適用。
- 停止受影響的伺服器的運作。
- 關閉系統的部份功能。
- 移除用戶的使用或登入權。
- 繼續運作以採集更多的證據。不過這可能只適用於擔當非重要任務的系統（可以承擔相當程度的服務中斷風險或資料破壞），但這做法需要特別小心的處理和在嚴謹的監控下進行。
- 禁止任何人接觸電掣、儲存媒體和電話，以保護電腦證據。
- 評估繼續停止運作和停止時間超過可接受程度的風險。管理層應該考慮 IRT 的建議，決定是否啟動災難復原計劃。
- 知會系統擁有者最新的狀態，以獲得到他們的信任和令他們放心。

根除

根除的目標是完全排除或緩減保安事故的來源。在這階段，根據事故的性質和系統的要求，企業可能需要進行以下的行動：

- 停止或取消所有入侵者正在運行的程式，藉此趕走入侵者。
- 刪除所有入侵者製造的假檔案。系統管理員可能要先將這些假檔案儲存，以協助調查。
- 刪除所有由入侵者安裝的後門和惡意程式碼。
- 為所有作業系統、伺服器和網絡工具的保安漏洞安裝修補程式。企業應徹底測試修補後的系統才把它投入正常服務。
- 改正所有系統和網絡的設定，例如防火牆和路由器的不正確設定。
- 如果事件由病毒感染引起，企業應依照防毒軟件供應商的建議，在所有被感染的系統和媒體上刪除病毒。
- 確保後備系統沒有被感染，以避免使用後備系統復原時再被感染。
- 使用保安工具幫助根除事故的來源，例如使用保安掃描工具偵測入侵和使用建議的保安方案，並經常更新這些工具的入侵特徵資料庫。

- 更新所有登入帳戶的密碼，因為入侵者可能已經取得這些資料。
- 當系統支援人員不肯定重要系統的破壞程度，或太難完全清理受感染系統時，可能需要重新格式化所有受感染的媒體，然後將備份資料重新安裝。

復原

這階段的目的是將系統復原至正常運作狀態。工作包括：

- 進行損壞的評估。
- 從可靠的備份媒體，重新安裝受破壞的系統。
- 根據需要的優先次序，逐步執行原有的功能和服務，例如先恢復最基本或最多人使用的的服務。
- 確保系統成功地恢復至正常運作狀態。
- 預先通知所有有關機構和人士有關系統將恢復運作的消息，例如：網絡操作人員、網絡管理員、高級管理人員和其他參與應變行動的人士。
- 終止不必要的服務。
- 記錄所有進行過的行動。

事後的跟進

跟進的目的是從事故中汲取教訓，改良系統的運作。在事故發生之後應該儘快跟進，管理層、用戶和在現場的 IRT 都應該參與。

- 進行事後檢討，找出需要改善的地方，例如：檢討現行的設定和步驟是否足夠、檢討是否需要給予用戶更多培訓、決定是否需要由外來專家進行保安審計和決定是否就事故進行法律行動。
- 所有參與的人士應該對事後檢討分析報告提供意見。
- 向管理層提交一個包括改善建議的行政報告。
- 管理層應評估這報告，並選擇建議去執行，管理層應嗚謝或獎勵舉報事故和參與事故應變的人員。

跟進事故的下一步是回到事故應變循環的第一步「準備」，執行被選擇的建議，進行另一周期的持續改善工作。

辦公室數據保安須知

日常生活中，任何人都可透過流行的工具與技術，如流動電話、電子郵件、即時通訊服務、可攜式的儲存器及經無線網絡接達互聯網的能力，輕易地攜帶及處理大量數據。隨著攜帶數據的便利，要把關鍵的機構資料儲存到個人設備中，或利用公共訊息服務處理，有很多其他不當的方式使資料洩漏到公眾的領域。

數據的保護曾經依賴實體性的防禦或完全隔離原始數據的策略，也就是限制接達在大型主機系統、磁帶或磁碟上儲存的數據位元與字節。時至今日，這種策略已不足夠應付保護數據的要求，因此限制接達這種靜態的防禦方法並不適合使用於現代的商業實務上。現時，公用客戶端（電腦及流動裝置）能使用相容的介面標準與公司的服務溝通，所以只要有渠道和機會，任何人都可接達與轉譯任何來源的數據。

保護企業資料的小貼士：

意識與責任

透過教育與定期提示，讓內部工作人員充分意識到保護企業資料是共同的責任，是相當重要的。因此，資訊保安的重要性是不容忘卻與忽視的。每個僱員都必須要充分意識自己的責任、在資訊接達上的限制及任何可能造成保安事故的紀律處分。

UPM Finesse Classic Matt, 90 gsm

定時評估與政策

在作任何改變之前，企業應先評估建設在公司內各處的資訊系統及確認其必須改善的地方。同時，建立一個保安政策去管理隨之而來的指引與程序的發展是必須的，而且需要定期執行持續的評估，這使既有的程序能因應工作條件與新的技術作出更新與改善。

數據的分類

並非所有的數據都屬於相同等級的重要性或敏感性，為了善用資源，應該以公司數據的保安等級來作優先次序，把保安上所用的資源先集中在最重要的數據上。

接達的限制

軟件及機密數據的接達應該是僅能給予經過授權的員工。使用密碼或者權標這類型的認證方式在接達的保護上，是屬於較常見的技術，並且可根據使用者的角色，把不同的授權配置檔應用於不同使用者上。

審計追蹤是認證的另一個補充辦法，而且全面的活動記錄也能夠提供有用的資訊去改善保安措施的效率。數據加密對未經授權的數據接達提供了另一層次的保護。

流動裝置的保護

流動資訊處理裝置與儲存在其中的數據，不論是遭盜竊或者是在沒有人看管的情況下，都會很容易遺失。實體的防護方法中，使用防盜安全鎖是最常見的第一道防線。另外，還有額外的授權要求以防衛未經授權的接達，例如設定密碼。使用者應自行判斷在這些裝置上儲存保密資料的風險及必要性，更要定期進行數據備份。

網絡的防護

防止從互聯網的入侵或攻擊是一個很大的課題，例如防火牆及代理伺服器這些產品都已經可以提供某一程度的數據與系統保護。然而，每家公司的數據系統中不同的架構通常都必須受到評估，並設計出針對該公司營運所需的保護措施。企業應定期掃描硬碟與可攜式的儲存器，並即時更新修補程式、病毒識別碼特徵檔（virus signature pattern files）和惡意程式碼定義。

公用渠道的保安措施

公用通訊的渠道，如即時通訊（IM）、無線網絡的接達及公共網上電子郵件服務等，都有可能帶有公司的資訊。在辦公環境中使用這些公用渠道時，以下的控制措施是必要實行的：

1. 發展一套清晰的通訊使用政策，並發布這些訊息讓所有員工知道；
2. 考慮推行一個相當於企業的統一解決方案，而非使用公用通訊服務；
3. 在適當的地方實施保安保護系統；
4. 暫停使用一些不安全的服務，例如遠端啟動的錄影機。

電腦配備的棄置

當丟棄舊有的電腦配備或內存非揮發性數據的儲存媒體，便需要一個適當的程序去保證所有的資訊和數據都已經被刪除，例如對儲存媒體作實體破壞、覆寫資料，或是重新格式化。

員工個人物品的限制

在某些狀況下，企業應防止員工攜帶個人物品進入工作範圍，包括流動電話在內。此舉有助排除一些數據被竊取的機會，而重要的或敏感的數據可儲存於虛擬機器內已加密的資料夾，這樣操作上的數據便可自動加密。■

如果想了解更多有關資訊保安管理的內容，請參閱以下的資料：

資訊安全網

網址：www.infosec.gov.hk
電郵：webmaster@infosec.gov.hk
傳真：(+852)2989-6073
地址：香港數碼港道一百號數碼港一座六樓