資料來源：香港特區政府資訊安全網

提升企業資訊保安能力 保障中小企業珍貴資產

資訊是中小型企業的珍貴資產，即使是細小的資訊損毀或破壞，也有可能令企業在金錢或商譽方面帶來巨大的損失，例如遺失客戶個人資料，以致該資料被未經授權人士使用，該公司可能會因而招致業務損失及法律訴訟。

在現今競爭激烈的商業環境中，業務的成功實有賴顧客的信任。一家公司的可靠性有助提高業務競爭力，從而在市場中茁壯成長。企業具備保護客戶資料的能力，即企業資訊保安的能力，才能取得顧客的信任。今期《香港印刷》為中小企重點介紹一些需要關注的重要範疇，並提供有關工業和技術上的指引，藉此提升其可靠性和資訊保安能力。

重要資訊的接達控制

中小型企業應按照需要知道 (need-to-know) 的原則來發出資料接達權，否則就會面對以下的保安風險：

- 未經授權員工可接達到敏感資料，例如薪金帳冊紀錄。
- 也許有人會破壞企業的資料。
- 也許企業已違反個人資料（私隱）條例。

接達控制

企業可在資訊科技系統中設定及應用接達控制政策，以允許特定人士接達至特定資料類別，例如人事部門的員工可接達薪金帳冊資料，而市場行銷部門的員工則無法接達。企業應按照需要知道原則來發出接達權。

保安貼士

- 定期檢查及更新接達控制政策。
- 限制系統管理者和用戶的數量和領域。
- 依個別任務來發出接達權，而非依個別人員而發出。
- 分配給每個用戶獨一無二的用戶 ID。
- 教育用戶有關資訊保安的重要性，並經常提醒他們保安最佳作業實務。
- 一旦員工離職或更改職務，便應使其帳戶失效或移除相關的權力。
- 確定每個人接達系統時皆通過登入和登出的過程。如用戶端閒置了一段時間，系統應該有自動登出功能。
- 假如連續登入失敗數次，應使該帳戶失效。
- 使用難以猜測的密碼，學習如何適當地處理密碼。
- 考慮使用生物特徵認證技術，例如指紋、面部特徵辨識或智能卡技術。
- 學習如何棄置無用的設備，因為機密資訊也許會遺留在棄置設備中。

UPM Finesse Classic Matt, 90 gsm

尋求建議和支援

企業要學習所有必要的保安知識和技巧是不可能的事，因此應該學習如何使用其他有用資源，例如可參閱**資訊安全網**〈www.infosec.gov.hk〉上的實用連結。此外，香港政府中小企業發展支援基金資助的**香港資訊科技方案互動名冊**〈www.itsolution.org.hk〉可協助企業找到正確的 IT 合作夥伴，以提供 IT 解決方案和資訊保安服務。

假如企業決定將資訊系統或 IT 服務外判給第三者的服務供應商，便需要佈置適當的保安管理流程，以保護資料，同時也可降低外判計劃／服務的保安風險。

處理保安事故

一個周全的保安事故處理計劃對資訊系統的有效運作極為重要，而該系統的運作亦會對機構的整體運作造成影響。保安事故處理計劃能協助企業有系統地應付由保安事故所引發的連串問題，盡量減少損失和以更有效的方式解決困難。（另見《香港印刷》第 123 期報導）

定期備份

備份及復原的重要

備份是指在某特定時間保存一份數據的拷貝。「備份及復原」一詞，常指由某一位置傳送已拷貝的檔案往另一處，傳送時會在拷貝的檔案上進行不同操作。

有效的備份策略是數據保安必不可少的元素。備份是防止損失的最後防線。有效的備份有以下的好處：

- 在硬件故障或意外刪除資料時提供保障；
- 保障用戶免被入侵者在未獲授權的情況下竄改資料；及
- 查閱以往的備份可提供入侵者活動的記錄。

備份及復原的步驟

備份及復原可視為一個須反覆進行的循環工作及過程，期間須進行持續監察和控制。

步驟一：計劃及準備
步驟二：確定資產及備份的需求
步驟三：選擇及建立備份策略
步驟四：執行及監察備份策略
步驟五：復原及演習測試

保護企業電腦資產

電腦設備是公司的重要資產，通常都儲存了有價值的資料。因此，企業必須考慮以下幾點來保護電腦資產：

硬件清單

- 保存一份最新的電腦硬件設備清單，其中包含所有零件的詳細資料。
- 內容應包含中央處理器 (CPU)、隨機存取記憶體 (RAM)、硬碟容量、顯示器尺寸等等，並詳細列出有用的相關服務資訊，例如保證書有效日期、序號及服務聯絡資料等。
- 應制訂預防政策，以避免員工在未經許可下拿走電腦設備。

軟件清單

- 保存一份最新的軟件清單。
- 企業必須確定有足夠的軟件使用許可證，並提醒員工不要安裝自己的軟件。
- 在試用日期到達之前，應移除共用軟件。
- 企業需注意一些許可證會以許可證號碼或小商標的形式出現，並要將許可證保存在安全的地方。
- 根據版權條例 (Copyright Ordinance)，企業有責任確定在商業用途上，並沒有使用任何非法軟件。

資料備份

- 須緊記定期備份，以保護公司的資料。

棄置電腦設備

- 為了避免資料外洩，企業必須學習如何適當地棄置電腦或儲存媒體。
- 在棄置任何硬件時，應移除已安裝的程式，並刪除所有資料。

加強實體保安

實體保護企業的電腦設備是很重要的，就像其他所擁有的價值資產一樣。因此，企業可考慮以下工具或方法來保護電腦：

- 使用保安鏈條鎖上電腦
- 自動關閉門
- 窗戶鎖
- 房間之間的可上鎖門
- 保安門簾或百葉窗
- 警報器（確定每位員工都有自己的警報密碼）

伺服器的保護

- 確定伺服器和網絡裝置存放在上鎖的房間或櫃子中。
- 切斷未使用的互聯網連結。
- 執行火災及水災警報器系統。
- 確定放置伺服器的地方有足夠的通風及冷氣。

其他貼士

- 限制接達，例如伺服器室等敏感地區／區域。
- 記錄伺服器及個人電腦序號。萬一遇上偷竊，便可被確認及復原。
- 存放備份媒體在安全的地方，尤其是儲存敏感或關鍵業務資料的系統。
- 為所有公用設安排定期維修及測試，例如氣調節設備、火警探測及防火系統和備用供電系統等。

保護企業的網站

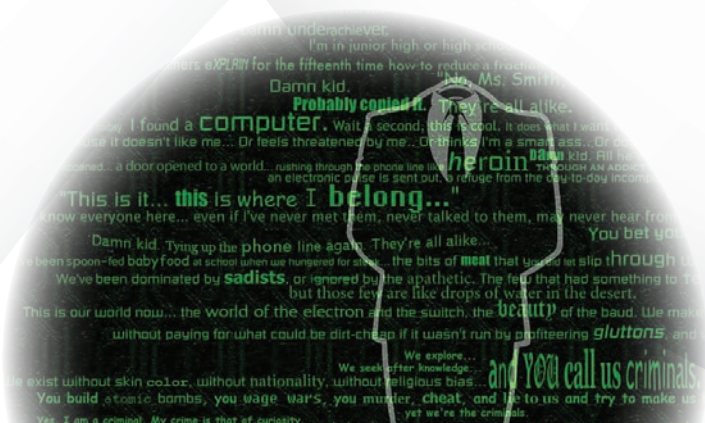
假如企業擁有電子貿易網站，就有機會面臨以下風險：

- **虛假買賣**：通常會造成企業因信用卡拒付 (Chargebacks) 的問題而損失收入。
- **詐騙網站**：有人設立看似公司官方網站的詐騙網站。
- **數據盜竊**：入侵者也許偷取企業的客戶資料，例如信用卡號碼。
- **入侵者攻擊**：入侵者的攻擊也許會造成網站功能的篡改或損壞。
- 因以上任何的風險而引致企業聲譽受損。

保護措施

假如企業親自管理電子貿易伺服器，而非向第三方服務供應商租用伺服器服務，就必須考慮以下重要事項：

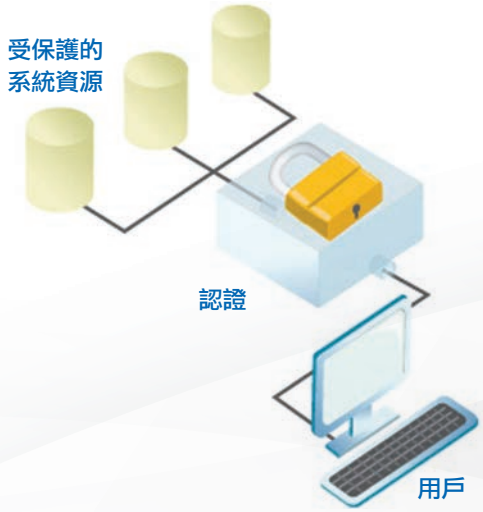
- 時常查看所使用的軟件的相關保安新聞，並確定正使用最新的修補程式。
- 安裝並啟動防火牆。
- 安裝抗電腦病毒軟件及抗惡意程式碼軟件。
- 使用嚴格的密碼。
- 每天檢查電腦系統和網站伺服器保安記錄。
- 檢查每日的交易記錄，留意是否有可疑活動。
- 不要儲存客戶資料及任何信用卡資料於公共電子貿易伺服器。
- 當執行數據傳送、處理或儲存時，要加密敏感的數據，例如啟動安全通訊端層 (SSL)。
- 定期執行保安評估及審計。
- 保護知識產權。企業的網站內容也許會在未經同意下而被他人偷取，例如圖像，因此可考慮在圖像上加入水印圖案 (Watermark)。
- 定期備份。



UPM Finesse Classic Matt, 90 gsm

電子認證（商業用戶）

企業的業務需要「電子認證」嗎？



互聯網令提供信息和服務的模式起了翻天覆地的變化。為了保持競爭力，現時不少公司必須提供網上業務功能。為了將核心業務程序自動化，商戶更需要向客戶、供應商和員工等使用者，提供隨時隨地接達公司資料及應用系統。

為防止未獲授權人士接達受保護的系統資源，企業需要設立安全的認證系統，確定使用者的身分。

有哪些程序？

「電子認證」是電子交易中建立信任的重要一環，涉及兩大程序，分別是註冊和認證兩部份。

1. 註冊程序

「電子認證」的註冊程序一般包括兩大部分，分別為註冊和註銷。

註冊旨在：

- 確保聲稱的身分確實存在；
- 確保申請人的身分真確；
- 確保與身分相關的資料一致、準確及妥善記錄；及
- 發出憑證或記錄現有憑證的詳細資料。

註銷旨在：

- 於持有人身故、離職、更改名稱、終止業務或出現其他重大變動時，撤回及在有需要情況下更換憑證；
- 撤回和更換被竊／洩露的憑證；
- 於懷疑憑證洩露、被竊或有重大變動的情況下，暫時吊銷憑證；及
- 應客戶要求撤回憑證。

2. 認證程序

認證程序是識別和驗證企圖發送訊息或接達數據人士的身分，旨在：

- 檢查憑證在有關交易中是否有效；及
- 檢查憑證並無逾期、被註銷或撤回。

有哪些常見的威脅？

1. 註冊程序

一般而言，針對註冊程序的攻擊有三類，包括冒充身分、虛構用戶和註冊者惡意行為。

冒充身分 	攻擊者針對性或非針對性地以他人名義取得憑證。
虛構用戶 	攻擊者使用虛構的身分成為用戶。
註冊者惡意行為 	濫用受托的身分，以潛在用戶或虛構人士的身分，在機構內部建立或取得憑證。

2. 認證程序

針對認證程序的威脅也有四大來源：

竊聽者／中繼攻擊 	竊聽者會留意認證數據在網絡的執行情況，以便日後分析或截取真正使用者之間的訊息，然後以不正當手法取得權標冒充合法使用者。這方法經常與中繼攻擊一同使用，以惡意或欺詐手段重複或延遲有效的數據傳輸。
密碼猜測 	字典式攻擊是黑客盜取密碼的最常用手法，入侵者會逐一嘗試將字典中各個詞彙和名稱用作密碼。透過程式，每秒可猜測數以千計的字詞。
冒充檢查員 	攻擊者假冒檢查員，然後引導使用者透露其秘密權標。
騎劫者 	攻擊者佔用已認證的連線階段，然後假扮真正的用戶或資訊科技系統，以取得敏感資料或輸入／輸出無效資料。

3. 其他威脅來源

除了註冊和認證程序外，其他保安攻擊也可對使用者構成威脅。

- **仿冒詐騙／假冒網站**：攻擊者使用偽冒由合法機構發出的虛假電郵訊息，要求受害人提供帳戶識別碼、密碼等敏感資料，或提供欺詐網站的連結，讓受害人輸入敏感資料。
- **黑客入侵**：攻擊者利用電腦系統的漏洞，盜取個人資料、密碼等敏感資料，以作出進一步攻擊，例如冒充身分或控制帳戶。
- **跨網址程式編程技術**：黑客在合法網站安裝惡意程序代碼或手稿程式，當受害人瀏覽網站時，惡意手稿程序便會盜取敏感資料，或將受害人轉接至與合法網站相似的欺詐網站。

甚麼是「保證等級」？

「保證等級」是註冊及認證程序的信心程度，詳情如下：

	定義	例子
第一等級	對聲稱的身分沒有信心或信心極低。 此「保證等級」適用於洩露不會構成風險（或風險極低）的情況。認證機制只可保證是同一使用者接達服務、交易或數據。	一名客戶使用自行登記的使用者識別碼，用以建立個人化網頁或收取電子通訊，未獲授權接達識別碼的第三者可能會推斷出個人喜好的資料，但風險一般很低。
第二等級	對聲稱的身分有中等信心。 此「保證等級」適用於洩露會構成低風險的情況。	客戶須進行認證以查看交易的處理狀態，如應用程式並無披露敏感資料，相關的風險便不高。
第三等級	對聲稱的身分有高度信心。 此「保證等級」適用於洩露會引致中等風險的情況。	遠程接達病人的病歷或財務帳戶，並涉及敏感的個人資料。
第四等級	對聲稱的身分有極高信心。 當洩露會引致高風險時，便需要此「保證等級」。	未獲授權接達會洩露調查或妨礙偵測刑事罪行。

UPM Finesse Classic Matt, 90 gsm

電子認證系統架設流程

以下是商戶架設安全「電子認證」系統的一個建議流程。

1. 評估風險

風險評估是找出需要哪種認證方法和安全措施的第一步。風險可按照保安事件發生的機會和影響作評估，這可以是財務上的風險，包括錯誤執行或延誤執行而引起的即時、直接或間接損害。此外，亦可以與喪失機密性或私隱、損失名譽或盜用身分有關。

以下列舉常見的影響類別，以供參考。因應個別服務性質或業務要求而產生的額外影響，將需要另作確定。

- 令任何人士產生不便、憂慮或引致其地位或名譽受損；
- 令任何人士蒙受金錢損失，或帶來業務上的責任；
- 向未經授權的第三方發放個人或商業資料；
- 危及任何人士的人身安全；
- 協助展開或妨礙偵測民事或刑事罪行。

影響的程度介乎全無至高度，潛在影響的程度可大致分類如下：

- **沒有影響**：沒有可以衡量的影響。
- **低度影響**：有限而短暫的影響。
- **中度影響**：嚴重的短期影響，或有限的長期影響。
- **高度影響**：災難性、嚴重或非常嚴重的長期影響。

2. 釐訂「保證等級」

以下的評估參照表載列出不同「保證等級」可以承受的最大影響，每個類別的潛在影響程度，與可以承受影響的適用「保證等級」是相關的。按照此對照方法得出的最高「保證等級」，將會成為指定服務或交易的整體「保證等級」。

潛在影響	可以承受的最大影響			
	第一保證等級	第二保證等級	第三保證等級	第四保證等級
不便、憂慮、地位或名譽受損	低度	中度	中度	高度
金錢損失或法律責任	低度	中度	中度	高度
未經授權發放個人及商業資料	沒有	低度	中度	高度
任何人士的人身安全	沒有	沒有	低度	中度
民事或刑事罪行	沒有	低度	中度	高度

舉例而言，如果影響類別的所有評級均為「低度」，有關服務或交易便需要以第三保證等級作為整體的保證等級，因為第二保證等級不能承受「任何人士的人身安全」類別的「低風險」。

3. 釐訂要求

每個「保證等級」的基本要求（註冊和認證）詳情如下：

	註冊要求	認證要求
第一等級	此「保證等級」並無身分證明或設置註冊資料記錄的要求。使用者的身分聲明可毋須經過核實便獲得接納。	第一等級雖無特定的註冊要求，但認證機制應提供若干保證，以確定同一使用者正接達服務、交易或數據。 可供配備作第一等級的認證技術也有不少，包括使用簡易的個人辨認號碼或密碼。
第二等級	對於風險相對較低的日常業務交易，此「保證等級」已能提供足夠保證。在許多情況下，註冊程序可透過聯機而毋須親身進行。 程序確保申請人的基本身分資料得到檢查及核實。身分資料最低限度應包括全名及其他可核實資料，用以證實該申請人的身分。註冊資料的記錄亦應置存。	第二等級的保證依賴安全認證規約，以確立使用者「控制」權標的證據。 可供使用於加密網絡連接對話的認證技術也有不少，例如使用管理密碼權標（受密碼政策規限）。應實施像「加密」和「密碼政策」等的措施，以免受到偷聽者、中繼及密碼猜測的攻擊。
第三等級	申請人需要經過核實實質的身分證明，包括在某些情況下申請人須親身出示身分證明以完成註冊程序。除了該身分需確實存在之外，通常還需要提供至少有效及通用的一些憑證或文件以作身分確認。 需要核實的身分資料最低限度應包括全名、出生日期、目前住址和身分證明文件（例如護照或香港身份證）的識別號碼。應置存的記錄包括經過核實的資料、已採取的步驟和過程中已審查文件的副本。	在此「保證等級」，保證是建基於「擁有」認證權標（硬件或軟件加密權標）的證據。 可考慮的認證方法包括數碼證書或限用一次密碼。也應採取措施免受偷聽者、中繼、密碼猜測及核實模仿者的攻擊。
第四等級	除申請人必須親身出示資料以完成註冊程序外，此「保證等級」的要求與第三等級相若。除了該身分需確實存在之外，通常還需要提供至少有效及通用的一些憑證或文件以作身分確認。 需要核實的身分資料最低限度應包括全名、出生日期、目前住址和身分證明文件（例如護照或香港身份證）的識別號碼。應置存的記錄包括經過核實的資料、已採取的步驟和過程中已審查文件的副本。	第四等級的認證是建基於透過加密規約「擁有」密碼匙的證據。除需要「硬體權標」外，第四等級的認證與第三等級相若。 「硬體權標」應採用經國際標準核證的硬件加密模組，不能輕易複製，而且必須用密碼或生物測定學才能解鎖。藉著採用「硬體權標」，此「保證等級」可確保有良好的遠程雙重認證。 憑證必須在限定的時間內有效，而憑證的撤回狀況必須於交易時檢查。除了第三等級的保護措施外，系統應在設計上能防止未授權者接達到載有正確客戶驗證資料的數據庫。

UPM Finesse Classic Matt, 90 gsm

4. 實施保護

根據對註冊及認證程序所釐定的要求，實施可應用的認證方法及適當的措施，以減低相關風險或影響。

企業應注意，資訊系統的整體保安取決於多項因素。若果單純依賴認證權標設備作為唯一途徑，這不一定可確保或改善保安水平。在設計安全資訊系統方面，企業也可採用其他舒緩辦法，而以下保護措施尤其重要：

- 實施適當的技術措施，例如抗電腦病毒程式、防火牆、密碼匙管理等，以保護相關的操作環境；
- 經常追蹤系統活動、警戒訊息，用以識別可疑的活動；
- 經常獲取最新的保安消息、保安事件、安全漏洞、安全威脅及攻擊的報導；
- 採用良好的資訊保安慣例；
- 透過不同渠道，例如刊物、官方網站、官方聲明，直接通知使用者有關敏感的個人或帳戶資料在通訊或收集方面的政策或防預措施，例如在網站刊登聲明，表明將不會發放連接到網站登入網頁的電子郵件；
- 將不會透過電子郵件或電話要求使用者提供個人或帳戶資料；
- 提供通訊渠道處理使用者通報的保安事件；
- 教育使用者須遵從的良好保安慣例。

此外，各參與方（例如使用者、技術支援、使用者支援、管理層）應明白本身關聯的角色和責任，並需對其行為負責。

5. 監察、報告及審核

定期監察及記錄機制是應予以確立的重要元素，以便在處理保安事件時能取得足夠資訊及作出適當安排。

日常操作數據（例如應用程式的審計追蹤、事件歷史、誤差記錄、接達記錄或授權數據）應妥善記錄及備份，從而支援事件處理或其他所需的保安程序。此外，持續的審核和評估應融入整個系統的運作中，用以考慮到技術方面的進展和確保採用適當措施，來應付相關的新要求及變動。■

如果想了解更多有關資訊保安管理的內容，請聯絡香港特區政府資訊科技總監辦公室製作和管理的「資訊安全網」：

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