提高智能手機資訊保安警覺推廣活動

《智能手機資訊保安實用電子指南》

資助機構:

「中小企業發展支援基金」撥款資助
Funded by SME Development Fund
工業貿易署
Trade and Industry Department

主辦機構:

WTIA 香港無線科技商會 SINCE 2001

執行機構:

Hong Kong Productivity Council 香港生產力促進局

關於香港無線科技商會(WTIA)

香港無線科技商會是於2001年在香港註冊的非牟利機構，旨在為香港無線科技界提供合作平台，促進行業的發展與成長。商會的宗旨包括：

- 代表無線科技行業向政府及國際組織發表意見，維護業界權益
- 推動香港無線科技應用的發展，使用及認知
- 促進業界不同公司間的溝通及合作
- 提升在無線科技應用方案中軟體及硬體的專業標準

WTIA現有超過150個來自本地及外地的公司會員，包括流動網絡營運商、流動器材生商、軟硬體經銷商、系統集成商、無線應用開發商，流動內容供應商等。

WTIA經常與政府、行業商會及商業機構合作，實行了許多有意義的專案計劃和籌辦過很多重要活動。

香港無線科技商會的網址為：www.hkwtia.org

聲明: 在這本小冊子上並沒有推薦任何技術、品牌、產品或服務，敬請留意。

有關本小冊子計劃

本項目是由「中小企業發展支援基金」撥款資助。實用電子指南是結合資訊保安專家、應用程式(Apps)開發商、流動網絡營運商及保安工具供應商就智能手機資訊保安所發表的意見。指南綜合多種智能手機風險，提供實際的操作步驟，減少企業使用智能手機的風險。指南亦提供範例模板，幫助中小企制定公司內部的智能手機保安政策。

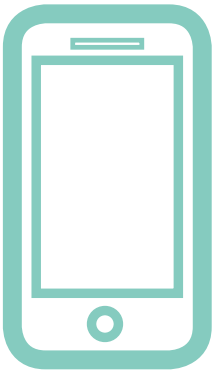
本項目的受眾為所有香港中小型企業，所有行業皆適用。香港有29萬家中小企，為約120萬人提供就業機會，佔本港總就業人數的48%（不包括公務員）。當中，有48%受訪人士（cellular-news, 2010年6月）聲稱擁有智能手機，並會使用其電子郵箱、互聯網及辦公應用功能。因此，本項目將有超過57萬受惠人士。本項目將為中小企帶來以下好處：

- 提高本港中小企及社區對智能手機保安之意識。
- 提高本港中小企的競爭力：中小企可在毋需擔心數據安全的情況下，於日常業務運作中有效地運用智能手機。
- 降低本港中小企採用智能手機保安措施的門檻：缺乏有關技術背景和資源的中小企，將有機會透過本項目出版之實用指南，就數據安全問題訂立相應的規範和措施。

目錄

1. 日益普及的智能手機

使用智能手機對企業帶來的好處



智能手機已經無處不在，它的普及性亦不斷擴大。據市場調查機構Gartner對個人電腦使用的預測，到2013年，智能手機將取代電腦成為全球最常用的網絡連接設備。許多人都體驗過智能手機的便利，世界各地的企業亦同樣瞭解智能手機可以給企業帶來的好處。智能手機容許員工隨時隨地存取業務資料、業務應用程式和供應商或合作夥伴的資料，提高體通訊能力。

企業感受到智能手機的好處包括：

- 若企業有訂立智能手機策略，便可為對這方面有認識的員工提供網絡連接，使他們可以在企業外部讀取電子郵件、企業文件和其他資料。這還有利僱員在外地完成工作，提高其生產力。

- 在任何時候都可回應或解決客戶的問題。有使用智能手機管理策略的企業，都確認客戶的滿意度得到顯著改善。

- 有效地採用智能手機，可以為企業提供更大的靈活性，尤其是面對不同時區或辦公時間的挑戰，和改進解決問題的「周轉時間」(turnaround time)。

- 智能手機能讓員工在旅途上，亦時刻與企業保持聯繫。

2. 智能手機上的威脅

一般智能手機用戶，都習慣在同一部手機上進行工作和個人活動，這容易對企業的保安造成威脅。智能手機用戶可能會丟失、被盜、或更換手機。強勁的智能手機存儲能力亦使企業內部文件和敏感資料更容易被廣泛下載、存儲或被控制。免費下載的應用程式(Apps)鼓勵消費者試驗，但亦可能導致其感染惡意軟件的風險。當連接到我們控制範圍以外的網絡時，數據洩漏的潛在風險亦在增加。

智能手機上的潛在威脅包括：

- 智能手機的便攜性使它們很容易被竊取。手機被盜後，用戶可能會失去所有儲存的數據，包括個人資料、財務和企業數據等。更糟糕的是，富經驗的攻擊者有足夠時間可以擊破大多數手機的保安功能，讀取其中存儲的任何資料。

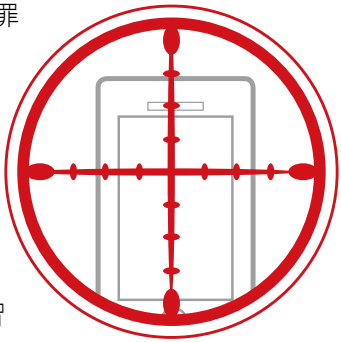
  隨更多智能手機在企業環境中使用，企業數據丟失和洩漏將更廣泛。越來越多敏感和專有數據，可能通過智能手機電子郵件附件、FTP上傳等丟失和洩露。智能手機也可能保留敏感或專有數據，在連接到無線網絡後，或者通過不安全的智能手機被洩漏。

  此外，只要找到沒有妥善放置的智能手機，任何人都可以盜取手機內的資料，如網絡接入碼、用戶名稱和密碼等，甚至在手機內安裝惡意軟件或間諜程式。

- 「越獄」(Jailbreak)或強行打開手機來改變其設定或功能（如改變移動服務運營商網絡上的限制）的做法，也帶來嚴重的安全威脅。例如，「越獄者」(Jailbreakers) 使用安全「Shell」（SSH）應用程式存取或改變這些設定時，往往忽略更新他們的「根密碼」(root passwords)，這就使他們很容易受到外界攻擊。此外，「越獄」的手機往往違反智能手機的服務協議，可能無法獲得系統或產品更新。同時，「越獄」的手機亦會失去大部分由手機製造商所提供的保安功能。

- 許多看似合法的應用軟件或應用程式(Apps)，是含惡意的。任何人都可以對一些最流行的手機操作系統開發應用程式，而移動服務提供商亦可能會提供一些可能沒有經過保安或質量評估的第三方應用程式。一些不受管制的應用程式可以存取手機內的個人資料或非法使用電話功能。

- 智能手機數量不斷增加，已成為罪犯有利可圖的攻擊目標。困擾傳統電腦操作系統的威脅，例如在電子郵件、社交媒體網站、遊戲、即時訊息和惡意網站傳播的惡意軟件，亦可以影響智能手機。智能手機可以擴大惡意軟件傳播垃圾郵件和釣魚訊息。因為智能手機提供比個人電腦更深入及更廣泛的通訊通道。用戶更容易接受偽裝成個人通訊的信息和文件。而且，用戶不容易偵測一個在手機小屏幕上顯示的網站是否一個假網站。同樣，手機感染惡意程式後的徵狀亦不明顯。



- 即使是合法的智能手機軟件亦可能受到入侵。手機軟件和網絡服務都可能有漏洞，就像一般個人電腦一樣。多年來，攻擊者利用手機軟件竊聽，摧毀手機軟件，或者進行其他攻擊。只要簡單的執行一個針對軟件漏洞的應用程式或網絡服務，用戶就有可能受到入侵。

- 使用電子通訊進行釣魚攻擊，誘騙用戶安裝惡意軟件或提供敏感資料，是個人電腦上常見的攻擊，也是黑客常用的伎倆，它對具備電子郵件功能的手機同樣危險。移動手機用戶也易受釣魚語音通話（vishing）和SMS / MMS訊息（smishing）誘騙。除智能手機外，這些攻擊也可以針對簡單功能的手機（即沒有先進的數據和無線通訊功能的手機）。詐騙者有時會誘騙用戶接受其手機上的欺詐性收費。詐騙者往往在重大事件發生後，增加他們的攻擊，製作自己（虛假）的通訊，使它們看起來像新聞報導或募捐慈善捐款。在2011年3月日本發生地震和海嘯後，垃圾郵件發送者也曾經使用同一方法誘騙用戶。

- 企業要管制智能手機很困難。智能手機可以透過無線連接到企業網絡、使用移動電訊網絡，甚或完全繞過企業的無綫網絡。他們可能會從網上下載惡意軟件，然後將它傳播到企業Wi-Fi網絡內。這使機構更難控制用戶與他們的智能手機對企業數據保安的威脅。

- 智能手機可能沒有安裝任何保安軟件。

3. 良好的智能手機保安做法

最佳的智手機保安做法，是要求機構使用成熟的保安技術及執行完善的智能手機政策。機構應制定、記錄和與員工溝通智能手機的使用政策，並配合相應的執行解決方案。政策文件的例子包括要求員工在他們的智能手機上設置強密碼，並在一旦遺失時立即向企業報告。執行解決方案的例子包括使用適當的保安技術，識別及驗證用戶身份，強制在智能手機上安裝保安軟件及保安設定等。以下是一些保安政策和技術的最佳做法。

3.1 企業的智能手機保安政策

訂立智能手機的保安政策刻不容緩，這對機構的保安性和是否合乎規定發揮關鍵作用。機構必須建立安全的移動保安環境，和使用智能手機的資料保護政策，它們要確定哪些政策是重要的，和為什麼要訂立這些政策。首先我們必須對智能手機使用所帶來的風險，有清晰的認識。

- 機構需要建立有效的政策，它包括對智能手機使用者明確的要求和期望。機構需定期教育所有用戶關於這些政策的內容，並更新他們如何應對不斷變化的智能手機保安環境。

- 作為既定的政策的一部分，適當的技術是必需的，如「移動設備管理解決方案」(Mobile Device Management solution簡稱MDM)的實施和執行，和部署企業智能手機保安工具，例如手機短訊、企業電子郵件和對智能手機上的敏感數據進行加密的工具，針對惡意軟件、垃圾和釣魚郵件、惡意應用程式(Apps)的手機保安軟件；防盜、遙距刪除丟失或被盜的智能手機的解決方案等。

3.2 手機安全

3.2.1 在手機上存儲的數據

我們要仔細考慮需要存儲甚麼資料在設備上。因為只要有足夠的時間、經驗，和接觸手機的機會，任何攻擊者都可以獲取手機上存儲的資料。所以我們要評估哪些地方存儲了重要數據，並評估一旦這些數據丟失或洩露出去，可能對機構造成的損害，以實施相應管制，減輕風險。

3.2.2 手機保護

智能手機上可以安裝的的保衛設施和軟件包括：

- **防火牆** - 阻止對不請自來的入侵者
- **防毒軟件** - 檢測和清除設備上的惡意軟件
- **反間諜軟件** - 防範間諜軟件的入侵
- **反垃圾和反釣魚郵件** - 過濾有害資料和電子郵件
- **入侵預防** - 檢測和阻擋企圖入侵襲擊
- **加密** - 保護智能手機上的數據和通訊

3.2.3 備份和復原

備份和復原智能手機內的資料，是一個全面安全配置的重要組成部分。許多智能手機操作系統廠商已經提供了備份和復原軟件供用戶使用，但這些功能通常要需要由用戶自行啟動。另外，用戶還可以安裝其他的商業產品進行備份和復原的工作。

一些產品或網絡供應商亦提供雲端備份服務，這些備份的工作可以在互聯網上自動完成。

備份和復原的設施應該能夠在預定的期間，通過互聯網或桌上電腦連接的智能手機進行數據備份。用戶可選擇備份的內容，並能夠在需要時復原所備份的數據。

用戶亦應該定期測試備份的資料是否可以完整復原。

用戶亦可透過智能手機和桌上電腦的同步功能做備份。

3.3 傳輸數據的保安

3.3.1 遙距訪問 (Remote Access)

黑客可以在用戶傳輸數據時，窺探設備上沒有加密的數據。例如，黑客可能在咖啡室，窺探他人的手機並接收未加密的數據，或者透過無綫網絡撈取未加密的資料傳輸。所以用戶在公共場所時，用戶應該通過「虛擬專用網」（Virtual Private Network，VPN）存取企業重要或敏感的數據。

「虛擬專用網」是指智能手機，與安裝在企業網絡的VPN網關或服務器之間的安全連接。當智能手機和VPN網關之間建立起VPN隧道，該隧道所有的通訊都是加密的。這種加密為智能手機和企業網絡之間的數據，提供安全交換。

如果你已經在家中的桌上電腦使用VPN連接到企業網絡，那麼類似的技術也可應用於智能手機上。經加密後的數據通訊內容，即使被黑客截獲和竊取也不能被輕易解密。

為了減省為不同的智能手機操作系統（如蘋果iOS，谷歌Android，諾基亞Symbian和微軟Windows Mobile）設立、管理和更新不同的的保安解決方案，機構可以部署一個集中的「安全連接層虛擬專用網」（SSL VPN）的網關。SSL VPN門戶網站可以提供基於網頁訪問的身份驗證和加密的網絡資源分配，減少對技術支援的需求。此外，機構亦可以和防火牆技術連結，形成清潔的VPN解決方案。SSL VPN在建立授權的門戶網站時，可以使數據管理有更嚴格的控制，同時為企業網絡提供卓越的安全和惡意軟件保護。

在SSL VPN門戶訪問的同時，機構也可以利用遙距訪問(Remote Access)技術的查詢能力，在設備和用戶身份的基礎上，確定什麼級別的訪問是適當的。一個有效的安全遙距訪問解決方案不應對所有連接都授予同樣的信任，應就手機的不同保安情況（包括類型、使用的軟件、該用戶在企業內的信任水平等）有不同的設定。一旦保安情況已經確定，解決方案應指定和強制執行適當保安政策水平。通過限制用戶存取和下載敏感數據，可減少或消除廣泛的數據洩漏威脅。

3.3.2 使用Wi-Fi無綫網絡

智能手機都設有先進的Wi-Fi功能，使它們能夠連接上公共和私人網絡。智能手機的用戶可以在公共場所，如咖啡室、機場、酒店、私人網絡等連接到網絡，其中包括企業和家庭的Wi-Fi網絡。

有些Wi-Fi網絡是開放的，用戶不需要任何身份驗證，就可連接到他們的網絡上。 所有用戶只需要知道這個開放網絡的網絡名稱（或確定的SSID），就可連接到它的服務上。這類型網絡的保安風險較大。

智能手機用戶應避免連接上未知的Wi-Fi網絡，或使用未經加密的公共Wi-Fi熱點。攻擊者可以設立一個假的Wi-Fi熱點或巡視不安全的公共Wi-Fi網絡來攻擊手機。此外，自己家中的Wi-Fi網絡亦應該有加密設定。

大多數智能手機都配備了Wi-Fi功能，故此有必要建立智能手機無線接入保安。 「無線局域網」（WLAN）的保安，應設定為只適用於已知道的用戶通過Wi-Fi連接到企業網絡上，並配合傳輸加密的WPA2。為了更安全，無線局域網還需要其他保安功能，例如入侵防禦，防病毒和反間諜軟件技術等。

智能手機用戶應在他們工作或不在家時關閉家中的Wi-Fi，以避免其他人進行「中間人攻擊」(Man-in-the-Middle attack)。如果已經在你的桌面電腦或筆記本電腦進行加密，同樣可以在智能手機上執行。我們也可以在傳輸數據前，在電腦或手機上進行加密，以確保內容不會容易辨識。

3.3.3 使用藍芽 (Bluetooth)

手機的藍芽也可能受到「中間人攻擊」的影響。我們應儘可能使用加密的藍芽手機。在一般情況下，不使用藍芽時，應關閉它的設定，同時應將藍芽功能設置為「非發現模式」(non-discoverable mode)。因為若被設定為「發現模式」(discoverable mode)時，附近的其他設備亦可以發現它，對手機進行攻擊。在非發現模式時，你的藍芽功能設備就不會被其他未經認證的設備發現。

3.4 手機管理

3.4.1 實物安全 (Physical Security)

在公開或半公開的地方，尤其要小心手機的安全。手機的便攜性使得它們很容易丟失，而智能手機的價值亦使它成為熱門的盜竊對象。我們亦不要讓手機在無人看守的情況下，被他人安裝惡意軟件或間諜程式。

一些保障實物手機安全的基本原則包括：

- 確保手機在任何時候都在你的控制範圍內。
- 確保手機上的數據是加密的。
- 不要把從手機借給第三者。

在棄置手機之前，刪除所有存儲的資料。我們可以在製造商的網站上了解如何安全地刪除數據的資料。手機供應商也可能提供服務，協助我們安全地刪除手機上的數據和資料。

如果智能手機丟失或被盜，我們應：

- 立即向你工作的企業/或移動服務提供商報告遺失。如果你的手機用於存取企業數據，應通知你的機構有關數據的內容。如果丟失的手機是你個人的，亦應盡快聯絡你的移動電話服務提供商，以防止他人惡意使用你的手機，減少欺詐性收費的損失，例如撥打國際長途電話。

- 需要時，可向警方報告丟失或被盜。

- 如果你使用的手機可以連接到企業網絡或社交網站，應盡可能刪除你手機上存儲的重要資料。這做法可能需要聯繫你的技術部門，撤銷連繫的保安證書或即時登錄到網站上更改密碼。

- 如果可能的話，遙距刪除你手機上的數據。一些移動服務供應商可以提供遙距刪除服務，可以協助你遙距刪除手機上的所有數據。

3.4.2 管理和控制

在可能的情況下，安裝一套「移動設備管理解決方案」(Mobile Device Management solution，MDM)，提供集中管理和實施企業訂立的保安政策、密碼要求、硬件和設備控制、證書管理、報告、問題警告等。

不要連接可疑的電子郵件或短訊發送的鏈接。這種鏈接可能會引領你到惡意網站，感染惡意軟件。留意軟件產品的評價，選擇信譽良好的解決方案。學會如何識別釣魚郵件或其他保安陷阱。

減少讓其他人知道你的手機號碼。攻擊者會有系統地從網上收集手機號碼和相關資訊，然後使用這些號碼為攻擊的目標。

關掉那些目前不用的接口，如藍芽，紅外線或Wi-Fi等。攻擊者可以利用軟件中使用這些接口的漏洞進行攻擊。

「越獄」的手機構成額外的風險。「越獄」過程本身就是在手機中加入漏洞，開發這「越獄」程式的組織不會確保他們沒有加載其他惡意軟件在程式內。「越獄」手機亦增加了企業保安環境的風險，因為這程式可以報告錯誤的資料給設備管理系統和其他保安工具。確保企業政策禁止在企業環境中使用「越獄」手機，安裝設備管理工具，以識別並報告「越獄」設備。

我們要教育智能手機的用戶有關使用地理位置(geo-location)和其他相關「功能」 的風險。注意應用程式共享位置資料可能對你和你的機構構成的風險。用戶應了解和決定是否分享這些位置資料。

3.4.3 實施修補程式更新

智能手機操作系統供應商、硬件製造商或移動網絡供應商都不時為智能手機提供操作系統更新。這些更新包括保安方面的改進，修復智能手機上的漏洞，或加強手機的保安功能。機構或個人用戶應定期檢查可用的更新，並在可能的情況下執行這些更新。

3.4.4 配置和設定

選擇智能手機及網絡供應商時，要考慮其安全性功能及服務。例如該手機是否提供檔案及文件加密，供應商是否能提供找尋遺失手機和可遙距刪除設備的能力，有沒有可偵測及刪除已知的惡意應用程式的能力，並有提供手機存取驗證功能，例如密碼設定。如果要備份手機數據到個人電腦，亦可尋找一個具有加密備份的選擇。如果打算使用VPN連接到企業的網絡，可了解手機是否可以設定VPN，亦可要求供應商提供支援保安證書的認證。

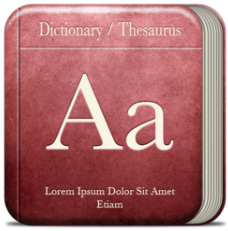
配置更加安全的手機設定。許多智能手機都有密碼功能，以鎖定裝置，直到輸入正確的PIN或密碼。啟動此功能，並選擇一個複雜的密碼。啟用加密、遙距刪除功能，安裝或啟動已安裝的的防毒軟件。使用PIN或密碼來保護你的智能手機。要定期備份數據。選擇「遙距刪除」，以便在手機丟失或被盜的時候，亦可清除手機內容。

配置網站帳戶使用安全連接。某些網站的帳戶可被配置為使用安全的加密連接（HTTPS或SSL）。啟用此功能可以阻止攻擊者竊聽網絡傳輸的內容。許多流行的電子郵件和社交網站，都有包括此選項。

3.4.5 報告事故

企業應建立適當的程序幫助員工報告智能手機的事故，包括丟失和盜竊、惡意軟件感染、保安攻擊和企業敏感資料外洩等。這些程序亦應包括在甚麼情況下提升到向管理層報告事件，或向香港電腦保安事故協調中心（Hong Kong Computer Emergency Response Team Coordination Centre - HKCERT）報告，以作進一步調查或採取復原方案。機構應中學習，提高保安防範和改善未來的保安實施。

3.5 智能手機應用程式 (Apps)



嚴格挑選和安裝應用程式(Apps)。在安裝前做一點應用程式的研究，檢查應用程式要求什麼權限。如果要求過度權限的應用程式，我們應要考慮不安裝這應用程式，它可能是一個木馬程式，或包含惡意代碼。下載應用程式和軟件前，應仔細閱讀隱私條款。此外，從陌生的供應商下載新的應用程式前，應等待該產品已被其他用戶進行測試後，留意別人對這應用程式的評論。

使用社交網絡的應用程式要格外小心。這些應用程式可能會發掘很多個人資料，並提供給其他機構。使用服務和顯示位置時，更要特別小心。不要過度分享社交網絡上的資料，要仔細考慮哪些內容正在與哪些人共享。

留意社交網絡中的漏洞。應限制員工在社交網站的曝光，並鼓勵他們不要分享個人或機構的資料，並密切檢討「朋友」的請求和發出的電子郵件。建議員工不要點擊他們沒有親自會見的人發出的電子郵件中的鏈接。

3.6 智能手機保安工具

3.6.1 工具的種類

企業應採取多層次的方法，保護智能手機。實施「智能手機管理解決方案」來管理保安政策，因許多設備管理解決方案可支援，允許/封鎖

特定應用程式。應使用加密的電子郵件解決方案，以防止惡意的應用程式把手機內容、企業電子郵件數據等複製到遙距位置。

市場上的移動保安方案可能包括以下幾類：防火牆、防病毒、反垃圾郵件、反釣魚、防盜、防入侵、家長監控和加密軟件。

3.6.2 工具評估

一些軟件程式的表現可能比別的更好，更容易使用。在決定哪些移動保安解決方案適合你和你的手機時，要留意你的需要和你的手機是否支援這軟件程式。一些評估標準包括：

- **有效性** - 保護能力的水平。無論它的外觀或附加功能如何，它應該有效地保護你的手機。優秀的手機保安軟件將整合更多功能，並提供實時保護。

- **特色功能** - 一個好的移動保安解決方案應可協助保護手機。用戶應評估自己的需求，並識別合適的方案，毋須超過本身需要。

- **易用** - 軟件應該使用簡單、直接、易於操作，接口亦應易於使用，以助用戶保護自己的智能手機。

- **安裝和更新** - 安裝應沒有困難。無論你是直接應用到手機，或將手機同步到個人電腦，安裝都應方便快捷。最新的保護是至關重要的，因此方案必須能盡快提供有效的更新。

- **應提供技術幫助和支援** - 應該提供在線幫助，並提多供多方面技術支援包括電話、電子郵件和在線聊天。

一些市場上流行的工具包括：

產品名稱	優點	缺點	備註
BullGuard Mobile Security	強大的家長監控。	不支援Symbian或Windows Mobile操作系統上，防火牆保護和垃圾郵件過濾器。	BullGuard Mobile Security的好處是它的家長監控能力，它可以支援多個設備的移動保安應用。 對大部份的操作系統，如Android，Windows Mobile，Symbian和BlackBerry等，提供支援。它還提供了防盜功能。
Kaspersky Mobile Security	Kaspersky主要偵測惡意軟件，被盜或丟失，亦可以用來尋找失踪的電話。	這軟件僅適用於Windows Mobile和Symbian智能手機。	Kaspersky Mobile Security 9是一個很好的智能手機安全軟件。. 它有助保持設備和數據的安全。它可以防禦移動惡意軟件，和實物盜竊保護。
ESET Mobile Security	提供實時保護，迅速從設備中刪除任何可疑文件。	沒有客戶服務的實時聊天支持。	ESET Mobile Security提供強大的防盜功能。提供先進的保護免受病毒，蠕蟲和木馬感染。這軟件還提供防火牆和防垃圾郵件保護，及有防盜竊功能
Lookout Premium	提醒下載的應用程式會在手機上存取甚麼資料。	缺乏顧客服務的一些支援功能。	如果你常常下載手機上的應用程式，這軟件最適合你。它可以保護你的私隱。這個軟件並提供備份，定期更新和防盜功能

Trend Micro Mobile Security	具阻止來電，家長監控工具和手機丟失保護。	此應用程式僅可用於Android上。	對Android智能手機來說，Trend Micro Mobile Security Personal Edition是理想的應用程式，如果你不關心防火牆保護，但需要家長監控，阻擋通話和訊息，和協助被盜或丟失手機的功能
F-Secure Mobile Security	強大的病毒和防火牆保護。	不提供垃圾郵件的保護。	F-Secure Mobile Security提高手機保安。保護你的智能手機免受病毒，蠕蟲，特洛伊木馬和其他移動惡意軟件的保護。
NetQin Mobile Security	有效的惡意軟件保護。	缺乏反垃圾郵件功能。	NetQin Mobile Security 獨特的功能使它成為一個很好的選擇。保護免受病毒，惡意軟件和其他威脅。這種手機保安軟件提供防丟功能，讓你從遙距位置來控制手機上的數據。此外，該應用程式提供出色的掃描功能和備份能力。
Webroot Secure Anywhere Mobile	內置的應用程式掃描器。	Webroot Secure Anywhere Mobile Premier只能用於Android設備，亦沒有防火牆保護。	這軟件提供基本的保障，但缺乏產品附加的特色，市場上有很多其他的產品，提供類似的功能。它的防盜竊的功能獨特，可以在地圖上找到手機的位置。使手機發出聲音，幫助尋找手機。並可以鎖定裝置，拒絕存取手機的所有內容。可刪除手機內所有個人資料。

4. 保護智能手機

注意：在不同版本的操作系統上，這些保護措施的步驟可能會有所不同。

4.1 屏幕鎖定你的手機

Android：進入 **位置與保安** > **設置鎖屏的設置**。
超時延遲(Time Delay)需另行配置　進入 **設置** > **顯示設置**。
Android還提供了一個連接點的輸入模式，以代替使用PIN或密碼。

BlackBerry：進入 **選項** > **保安選項** > **常規設置** > **密碼**

iPhone：進入 **設定** > **一般** > **密碼鎖**

Window Phone 7：進入 **設置** > **鎖及壁紙**

4.2 遙距定位，鎖定和刪除手機：

Android：沒有內置的遙距定位和鎖定功能，但有幾個應用程式可以提供這功能，如Where's my Droid。

BlackBerry：從App Store下載RIM的免費BlackBerry Protect。

iPhone：如果使用iPhone 4（iOS 4.2或更高版本），可以採取蘋果免費提供的Find My iPhone和MobileMe服務。

如果使用第三代的iPhone，便需要参加付費的MobileMe服務，使用Find My iPhone功能。

Windows Phone 7：進入 **設置** > **找到我的手機**，打開遙控器上的定位/鎖定/刪除功能，然後上windowsphone.live.com 網站

4.3 備份或同步手機的數據：

Android：目前有沒有一個完整的備份選擇，但Android智能手機運行版本2.2及以上的有備份手機的設置和應用程式數據到Google伺服器。

你可以進入 **設置** > **隱私** > **備份我的數據**，看是否提供備份解決方案。 如果你使用你的Android手機的聯繫人，日曆等的Gmail服務，在你同步時，資料會自動保存在你的賬戶內。

BlackBerry：從BlackBerryDesktop軟件可以備份BlackBerry設備。
BlackBerry Protect的應用程式/服務提供在線備份設備設置，包括書籤，日曆，聯繫人和短訊等。

iPhone：iTunes會在你每次插入你的iPhone同步時，建立內容備份。
你可以使用MobileMe的功能將同步在線存儲與任何Mac和/或PC選擇的重要數據。

Windows Phone 7：Windows Phone 7沒有提供手機備份，但當你同步時，某些數據和文件會保存在你的Windows Live帳戶內。

4.4 實施修補程式更新：

Android：進入 **設置** > **關於手機** > **系統更新**。

BlackBerry：連接到電腦，然後到BlackBerry Update頁面，點擊「檢查更新」（Check for Update）按鈕。

iPhone：連接到電腦上運行的iTunes，它會通知你是否有可用的更新。

Window Phone 7：有可用更新時手機會通知你，但你需要連接到電腦上運行Zune軟件進行安裝。

4.5 關閉藍芽發現模式 (Discovery Mode)：

Android：進入 **設置** > **無線網絡** > **藍芽設置** > **可發現**，取消該選項。

BlackBerry：進入 **選項** > **藍芽**，然後按一下BlackBerry標誌（菜單）按鈕。 選擇「選項」，設置「可發現」（Discoverable）「否」，再按下BlackBerry標誌按鈕，然後選擇保存。

iPhone：你不能明確地關閉藍芽發現模式(Discovery Mode)，但iPhone只有當你在藍芽設置頁面時才可以設定為發現模式的。 **設置** > **通用** > **藍芽**。

Window Phone 7：與iPhone一樣，Windows Phone 7只有當你在藍芽設置頁面時才可以設定為發現模式的。在你的藍芽設置頁面上選擇 **設置** > **藍芽**。

4.6 找到VPN設置：

Android：前往 **設定** > **無線和網絡** > **VPN設置**。

BlackBerry（Wi-Fi功能）：前往 **選項** > **保安選項** > **的VPN**。

iPhone：進入 **設置** > **通用** > **網絡** > **VPN**。

Window Phone 7：目前不支持VPN連接。

5. 保持更新

雖然智能手機帶來新的風險，但在企業環境中，智能手機卻可以提高生產力和士氣，有助吸引和留住人才。故使用智能手機的關鍵是治理、教育和提高認識。

為保護智能手機，你必須不斷掌握最新的威脅類型和解決方案。我們可以定期瀏覽下列網站，以獲取最新的資訊。除了這些中立的網站外，你亦可以到保安軟件產品供應商的網頁獲取威脅和產品的資訊。

- **Tech SANS (www.sans.org)** - SANS (SysAdmin, Audit, Network, Security)是保安資訊網站的先驅，提供專題文章，每週公告和警示，培訓，和保安漏洞資訊。其成員超過165,000個保安專業人員。SANS網站上提供的保安資訊，有很多移動設備主題的內容。

- **Infosecurity Network (www.infosecco.uk)** - 此網站集博客，事故報告，以及短小精簡的錄像，包括不少手機保安資料。

- **National Institute of Standards and Technology (Security Research) (csrc.nist.gov/groups/SNS/index.html)** - NIST國家標準與技術研究所是美國商務部贊助的機構，提供有關保安管理、標準及指引等文件。

- **ICSA labs (www.icsalabs.com)** - The International Computer Security Association (ICSA) 國際電腦保安協會有大量的專題文章，並可連接到其他資訊保安問題及有用資料的網站。

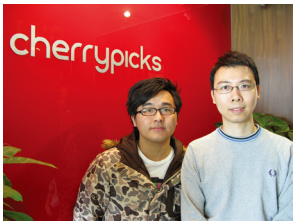
- **HKCERT (www.hkcert.org)** - 電腦保安事故協調中心 (Hong Kong Computer Emergency Response Team Coordination Centre) 提供智能手機事故處理服務，並會提供智能手機漏洞，並在其網站上提供指引及其他有用的資料。

- **GSM Association (gsmworld.com)** - GSM協會代表全球移動通訊行業，跨越219個國家，成員超過800多家企業，包括全球大部份移動營運商。網站涵蓋了一些很好的移動保安文章和議題。

附錄

A.1手機專家訪談記錄

受訪企業：Cherrypicks
受訪者：陳德高，袁展恒



1. 有哪些最新的智能手機資訊保安威脅值得關注？

2010年7月，Citi Group有一個名為”Citibank”的手機應用程式面世，內置了一個保安接口（security port）。但因為程式員疏忽，使用者所輸入的用戶名稱、密碼等個人資料將被儲存在手機內。如果手機被人盜取或遺失，用戶就有可能損失帳戶內的存款。

用戶經常都會將其個人資料、密碼等儲存到手機內，表面上並無不妥，但若遇上手機遺失，個人資料就會完全曝露，不法份子就有機可乘，盜用戶口。

這類於應用程式開發時疏忽而引起的保安問題可算是最典型的一種。站於開發者的角度，這問題相當大。因為一個網上遊戲發生事故，最多可能只是損失一些虛擬武器，但若網上銀行發生事故，損失就會相當大。

又例如一則於2011年12月的報導指出，若用戶使用iOS內iMessage的功能收發短訊，即使用戶將舊有的手機重新設定，並以新手機再登記iMessage功能，舊手機仍可收到相同訊息。換言之，若用戶將舊手機出售，則其新用戶仍可收到舊有用戶的訊息。如果訊息內容涉及生意

往來，則有機會造成商業秘密外洩。智能手機越趨普及，某些用戶會使用一些應用程式管理自己的帳戶。但當應用程式的設計或者手機本身檢測得不夠完善的話，就會發生很多保安的隱憂。

2. 可否提供一些智能手機資訊保安例子供《智能手機資訊保安實用電子指南》參考？

比較切身的例子有智能手機上的社交應用程式，如WhatsApp，LINE等。但現時的中小企大都不太在意這些保安問題。這類應用程式看似十分方便，不用繁複的設定便可與朋友互通訊息，但它們會自行將用戶電話簿內的資料上傳到應用程式的伺服器內，再由伺服器進行配對，找出朋友。

或許大部份人都會覺得沒有問題，但我認為此類應用程式在我不知情或不在意的情況下取得我電話簿內的資料，會引發其他有關保安和私隱的問題。

另一種是有定位功能的應用程式(location based application)如Foursquare，Facebook，Latitude等社交應用程式，很多人都會每到一個地方就會「Check-in」，但這些程式會否記錄用戶到過的地方再作其他用途，如轉售予第三方用作廣告用途或商業分析？這可能對用戶是一種風險。這些程式在用戶並無選擇下奉獻出其個人私隱，即使是自願下載的，用戶亦未必有足夠知情權了解此類運作。

第三種是現時約有5~10%的iPhone用戶會為其手機「越獄」，以使用App Store以外(如Cydia)的其他應用程式。但手機的防護性會在「越獄」後減弱，App Store以外的應用程式又可能含有病毒，容易令手機受感染。這類手機病毒輕則令用戶失去手機內的資料，重則會盜取手機內的資料作其他用途。

第四種是有關iCloud的功能問題。透過iCloud，用戶的電腦可立即同步處理手機的相片。雖然此項功能十分方便，但未必所有用戶都希望同步所有照片，而且如果電腦的保安工作不足，相片便多一分機會流出，危害當事人的私隱。據聞蘋果電腦方面亦正處理有關問題，但從這件事上可以知道如果開發程式時考慮得不夠周全，便有機會引致有關私隱的問題。

3. 對中小企來說，有哪些良好的智能手機資訊保安做法值得建議？

作為一個程式開發者，如果遇上要存取上述的敏感資料，如電話簿、位置等，都會盡量小心。例如該應用程式必須存取電話簿內的資訊，都會有兩個重點。第一，清楚地通知使用者該程式會存取電話簿；第二，一般的程式開發商都不會保留使用者的資料。

以上的做法是希望使用者可以安心使用程式內的功能，但使用者必須留意程式條款對其影響。

第二個建議就是關於Android Market。Android用戶下載程式前都會出現一個「通知」，提示用戶該程式會存取用戶甚麼功能。如果你下載一個遊戲，但它卻會存取你的電話簿、位置等不太相關的資料，用戶便須加倍留意。因為該程式可能有其他企圖，「掛羊頭賣狗肉」，刻意盜取資料，建議不要下載。一般開發商都不會存取不必要的資料。

4. 你會向用戶或中小企提出什麼智能手機資訊保安解決方案？

以用家來說，最基本就是為手機設置密碼。這樣即使手機遺失或被盜，都可保障手機內的資料不容易被盜取。另外iPhone以及Blackberry都有一個特別功能，可於手機遺失時遙距刪除手機上的資料，回復原廠設定，保障私隱。只是大多數人都以「事不關己」為由而沒有作相關的設定而已，其實只需幾個簡單的步驟已經可以完成設定，而且可於手機遺失時提供足夠的保障。

另外，不要為手機「越獄」和下載App Store以外的應用程式。

至於Android用戶，由於Android Market本身並沒有對應用程式作出審查，因此在Android Market下載應用程式會比較不安全。但Android Market會對程式開發商作認証，這樣用戶便可對開發商作出追查。

更重要的是千萬不要到第三方下載應用程式(如Cydia)，因為那些程式既沒有經過審查，又不能追查到開發者，又不知道它會存取手機內的甚麼資料，可算是全無保障。而且我認為手機比電腦更貼身，很多個人資料手機比電腦更齊備，因此用戶要更加留意。

市場上都有一些方案為中小企而設。以蘋果電腦為例，有一個名為「移動設備管理解決方案」(Mobile Device Management, MDM)的系統。這系統可讓企業透過MDM發放資訊予員工，系統亦可要求手機設置密碼、限制密碼長度、加密手機內的檔案、使用程式權限等的各類政策。好處是中小企可以此系統提昇保安水平，確保手機設置了密碼保護，即使手機遺失，被加密的檔案都不容易外洩。另一方面，中小企亦可透過MDM追蹤手機位置或刪除手機內的資料。

總結

市場上不同的管理系統功能雖然強大，但大多數員工手持的手機都屬於員工，企業要限制員工的私人手機會有阻力，為員工配置手機又會大大加重成本。中小企如果以Microsoft Outlook作為電郵伺服器，亦可做到要求手機設置密碼的功能。如果手機要連結企業電郵，就必須設置手機密碼，否則就不能存取企業電郵。這個方法相對簡單，而且亦可保障手機內的資料不會輕易外洩。

關於Cherrypicks

Cherrypicks是移動營銷、智能手機應用、擴增實境等新媒體科技的領導者。Cherrypicks不斷研發多種創新高科技的智能手機應用(iPhone、安卓、其他智能手機平台)、擴增實境技術(Augmented Reality)、雲端運算(Cloud computing)廣告宣傳平台。多間在香港交易所上市的大企業皆是Cherrypicks的客戶，包括香港上海匯豐銀行、港鐵、英國保誠保險、P&G、香港賽馬會、LVMH Group、Moet Hennessy Diageo Hong Kong Ltd、Estee Lauder、電視廣播有限公司、國泰航空、中華電力、中華煤氣、雅虎、諾基亞、Mercedes-Benz Hong Kong Ltd、香港旅遊發展局、香港貿易發展局、香港藝術節等。

Cherrypicks的總部設於香港，在印尼耶加達和中國北京，珠海亦設有分公司。Cherrypicks被「風險投資第一雜誌」的《Red Herring》選為”Red Herring 亞太區100強企業”之一。Cherrypicks是香港無線電科技商會創會會員，同時亦是Mobile Marketing Association 香港分會會長。Cherrypicks 獲獎無數，包括：亞太區數碼傳媒大獎、Mobile Marketing Association Global Award、香港資訊及通訊科技獎(最佳生活時尚大獎、最佳無間斷網絡大獎)、德勤高科技高成長中國50強、金帆廣告大獎、Global Mobile Awards。而多個Cherrypicks所研發的智能手機應用亦在各大公開比賽中屢獲殊榮。其CEO趙子翹先生和Cherrypicks是美國哈佛大學商學院研究個案之一(檔案編號：N9-807-106)。

不僅如此，Cherrypicks更研發並擁有多項高科技技術，包括：全球首個Location Based Augmented Reality (實景+定位+擴增實境技術)電腦視覺效果、臉部輪廓追蹤+擴增實境技術電腦視覺效果、圖像辨識技

術。同時，Cherrypicks與另一合作伙伴Dentsu Media在香港和亞洲推出iButterfly，是一種集創新、3D擴增實境科技、手機娛樂、收集優惠於一身的商業宣傳推廣服務。而在擴增實境技術方面，Cherrypicks與微軟緊密合作製作Kinect-based互動體驗予不同的客戶。

關於陳德高(Joseph Chan)

Senior Manager, User Experience and Software Development

- 超過10年移動應用程式開發
- 對手機設備有深入了解，熟悉智能手機應用程式設計
- 負責移動網站和智能手機應用程式之間的銜接環境設計，開發和管理的Cherrypicks移動廣告產品 - Town Check
- 管理、設計和開發各種應用，包括香港貿發局展覽，TVB Fun，雅虎香港和獲獎的港鐵移動應用程式。

關於袁展恒(Yuen Chin Hang)

System Analyst

- 超過8年移動應用程式開發
- 豐富針對iOS，Android，黑莓，休閒遊戲和信息檢索中的應用框架設計和JavaME開發經驗
- 帶領開發團隊
- 帶領各種應用程式，包括香港藝術節、飲食媽媽、港鐵移動應用程式的開發，設計和開發TVB Fun和Cherrypicks移動廣告產品Town Check。

受訪企業：天下網絡 (Newsky)
受訪者：范健文，麥泰然

1. 有哪些最新的智能手機資訊保安威脅值得關注？

我覺得最大的威脅是現在智能手機的數量很多。電訊管理局的數字顯示，超過50%最新的手機是智能手機，但大多數用戶並不了解智能手機內儲存了什麼資料。

以前我們可以自己安裝一些應用程式在手機中，但原來作業系統可能紀錄下我們的活動。有一個名為「Carrier IQ監控軟件」的事例很值得跟大家分享。Carrier IQ是一個媒介(agent)，安裝在一些外國手機裡，以前以為它只紀錄了網絡診斷、檢查接收訊號好不好、或者是用戶一些很簡單的習慣，例如應用程式關機時提交報告等。然而，事實是它紀錄了用戶的私隱資料，包括按鍵輸入、簡訊內容、訊息發送對象等。

可見我們買一部智能手機時，其實並不知道我們在手機內的活動有機會被第三者獲取。香港暫時未有這些事件報告，但在外國特別是在Carrier IQ這個事例上，已引起大家不安。因為我們用的手機開始越來越重要，我們會儲存相片、瀏覽很多網站、收發email、甚至做e-banking，這些紀錄一旦形成，就會對我們的保安構成嚴重影響了。

以前blackberry或windows mobile的年代我們有很多解決方案，而且當時的應用程式未有這麼發達。但我們現在上App Store見到的應用程式，一定比以前的windows mobile多很多倍，加上這些應用程式太容易太方便，很多用戶都可以自行安裝，開始引伸出用戶並不知道應用程式在手機背後會有什麼活動的問題。一個中小企資訊科技的經理，也要開始重視智能手機的保安需要。

此外免費Wi-Fi也許是一個陷阱。你不知道當中是否有加密，還是有一些黑客特意地放出一個沒有密碼的Wi-Fi給你使用，目的是用來盜取你的資料。

2. 可否提供一些智能手機資訊保安例子供《智能手機資訊保安實用電子指南》參考？

在香港，有關智能手機的威脅問題未算太嚴重。而一般在智能手機、手提電腦、平板電腦等設備的普通威脅，都是病毒攻擊、垃圾郵件、間諜軟件、資料盜竊、盜竊等。至於怎樣入侵手機去偷取資料，其實只是從以前的手提電腦或個人電腦的問題變為手機問題，入侵變得更加容易。

例如，美國休斯敦有一間做急凍食品公司，他們有很多在外工作的營業員，在下單時要第一時間用智能手機查看資料庫有沒有貨，或者要下載一些商品圖片，但員工全部都用不同品牌的手機型號，那企業在設計資訊科技措施就不能只針對某一品牌了。最低限度的資訊科技措施，需要員工為手機設置安全密碼。很多年前，軟件公司開發應用程

式可以透過網絡連接，把遺失手機立即還原到原廠設定；智能手機也可以設定如果錯誤輸入十次密碼，就會清除智能手機上的所有資料。

再用香港的例子。香港的保險公司的營業員可以在茶餐廳、快餐店、咖啡室與客戶見面，以前的做法是用手提電腦閱覽文件，頂多把計劃的收費計算出來。但現在產品的組合很多，保險從業員可透過手機進行下單等工作，所以假如手機遺失了，他們客戶的資料也一併遺失。因此，這類擁有大量智能手機用戶必須配合企業資訊科技措施來減少威脅。

3. 對中小企來說，有哪些良好的智能手機資訊保安做法值得建議？

對用戶來說，我覺得可以做的很簡單，就是不要貪方便或貪平而去把自己的智能手機「越獄」了，因為「越獄」同時瓦解了作業系統的安全性，失去監控。另外，只能在官方網站，如App Store或Android Market下載應用程式。

服務供應商的建議是在網絡設計及網絡器材上要有所準備。第一是面對每日不同的安全性威脅，第二是流量的增加。安全性威脅方面，企業資訊科技政策可要求員工的智能手機需要通過「虛擬專用網」(Virtual Private Network, VPN)才能進入企業的網絡。此外，我們可用防火牆去做一些很簡單的網絡保護，這5年來已有很多新世代的防火牆面世，它會經常下載最新的資料庫去加強保護手機，以預防最新的威脅。這是一個資訊保安資訊保安整合解決方案，所以兩方面都要並行。

流量方面，以前一個辦公室裡百多人大家都是用一些很普通的手機，有Wi-Fi的比率可能只有1-2%，但現在接近每一部都是智能手機，對應本身網絡的流量也比以前多了幾百倍。假如今天有50部、100部手機中毒，可能已經會立即攻擊自己的網絡。因此，一個可調節的防火牆或網絡器材，可給資訊科技經理/網絡工程師有充足時間去診斷問題。

4. 你會向用戶或中小企提出什麼智能手機資訊保安解決方案？

中小企都希望省錢，特別是下載免費軟件，以為只是安裝了就保護了自己，但那樣的防護是不足夠的。從企業的層面去看，坊間已有很多「移動設備管理解決方案」(Mobile Device Management, MDM)，但可能大家未很有信心去實行，因為實在太快太新。中小企一定要加強資訊科技政策，及徹底地實行在智能手機上，最簡單是要求員工為手機設置安全密碼，智能手機安全密碼可以設定為在輸入10次錯誤密碼後刪除手機資料。再者，若員工沒有在手機安裝防護軟件、沒有設定密碼就不能進入企業網絡，員工要查閱企業的資料，便必須接受這些條款。

另外，現在的技術可以透過服務供應商把遺失的智能手機上的資料刪除，還原原廠設定，有些更加可以把手機停用。每部手機都有序號，只要把遺失手機的序號告之服務供應商，其他人想換用也用不到了。

中小企需要跨平台解決方案，即無論是windows手機、iOS平台、Android平台也都能支援，提供最基本的防毒、防垃圾郵件等功能。這些解決方案看似昂貴，但事實上，現有的雲端解決方案，收費非常合理。

總結

無論是服務供應商、中小企資訊科技經理或者任何用戶，這三方面都不要認為智能手機的資訊保安不是他們的責任。智能手機發展太快，而每個應用程式所牽連的人亦很廣泛，所以我會給予三方的建議是，不要停留在舒適地帶裡，覺得現在的保安已足夠，在智能手機的技術層面上是永遠不會夠好的。最後，中小企要了解職員使用智能手機的需要，毋須覺得手機資訊保安要花很多錢，一些簡單的方法，例如防火牆，可提供最基本的保安需要。對用戶來說，不要太貪新鮮，寧願穩穩陣陣在官方網站，安裝一些穩定的應用程式便足夠了。

關於天下網絡 (Newsky)

天下網絡是一間擁有13年經驗的資訊科技服務供應商及產品分銷商，專長於網絡保安系統，為香港中小企提供價廉而優質的網絡安全解決方案。天下網絡了解到不同企業在網絡保安上的要求各異，所以特別重視售前的專業諮詢和售後的貼心技術支援，務求令客戶在發展互聯網業務上全無後顧之憂。

關於范健文(Eric Fan)

范健文(Eric Fan)是天下網絡的董事。在2010年天下網絡被Juniper Network 授予「香港快速增長公司」獎項，他本人亦獲頒「2010 Top SE」獎項。Eric同時任職通域存網有限公司，任技術開發負責人。他的團隊成立了通域網絡信息中心，成為.hk域名註冊商之一。在Eric及其團隊的努力下，UDomain已成為香港最大的網絡寄存公司，並擁有超過10,000個企業和個人客戶。Eric於網頁寄存和互聯網技術領域擁有超過十年經驗，不僅熟悉互聯網技術、網絡系統和網絡結構，而且熱衷於項目管理、戰略發展和培育公司新的業務。

Eric是香港無線科技商會執行委員會成員，並被委任為流動通訊和 Next Generation Network安全專家小組的召集人。

關於麥泰然 (Dellon Mak)

麥泰然 (Dellon Mak)在資訊科技界有超過20年實戰工作經驗。他畢業於美國及曾在美國費城的電腦公司工作，後遷移回港並在不同的機構服務，包括金融和科技。曾長駐北京、廣州等地，甚為熟悉中港商家所遇到的問題，並提供解決方案。在天下網絡，Dellon主要策劃及銷售網上保安、網絡設計和系統集成的業務。

受訪企業：電訊盈科流動通訊
受訪者：管紀東

1. 有哪些最新的智能手機資訊保安威脅值得關注？

一些mail-ware和病毒，令受感染的手機傳送出一些短訊，導致用戶被徵收費用，但用戶卻不知道手機曾傳送過訊息。以往亦有受感染的手機會撥電話到外國，令用戶需付國際長途電話費。

除以上問題外，智能手機亦可能因感染病毒致個人資料外洩。雖然直至現時為止，Android平台上已確認的病毒只有少於100個，未算嚴重。但這並不代表我們不需要防備。

我會將使用四種作業系統的手機歸類為智能手機：iOS, Android, Blackberry 和 Symbian。

iOS是一個較為「封閉」的作業系統，用戶只可於官方的「App Store」下載程式。「App Store」會對所有應用程式作出審查、篩選，而且開發程式受蘋果電腦開放多少所限，由於已開放的權限應不足以製作病毒，故此使用iOS的手機（iPhone）受感染的機會接近零，除非用戶為手機「越獄」。因為「越獄」後的手機可於其他地方下載未經審查的軟件，當中可能包含各種病毒，感染手機。

相比iOS的「封閉」，Android則是一個比較開放的平台。Android的代源碼是開放的，而且軟體開發套件不少，因此Android更有可能製作病毒。而且程式提交到「Android Market」並不需要審查，有問題的程式只會在例行檢查或被舉報時發現。基於Android是開放平台，程式可以更容易讀取到手機內的資料，如電話簿等。

Blackberry亦是一個「封閉」的作業系統。其已開放的功能比iOS多但遠不及Android，而且程式都需要經過審查，因此中毒機會都比較少。

至於Symbian，它的程式都需認證，否則會發出警告，通知用戶該程式可能會有問題。以往由於Symbian手機亦很普及，針對Symbian的病毒和手機漏洞較多，但現時Symbian手機使用率下降，相關保安問題亦已減少。

總括而言，就保安程度比較，iOS可算是最安全的一個，而Symbian由於使用率低，手機病毒已由最多的200個開始下降。至於即將推出的Window 7亦是一個較封閉的平台，相信保安程度應該不俗。Android為iOS外另一個使用率極高的一個作業平台，加上是一個開放平台，因此成為手機保安的一個隱憂。預期有關Android的保安問題會越來越多。

2. 可否提供一些智能手機資訊保安例子供《智能手機資訊保安實用電子指南》參考？

一般製作病毒的程式開發者，目的都是賺錢，佔全部病毒的百份之

五十。這些病毒會令開發者得到直接或間接的得益，如收取短訊費用、送出廣告或出售用戶手機內的個人資料等，但上述保安問題在香港並不常見。只是每年都會有一至兩宗用戶因手機中毒，不停發出訊息而導致損失的個案，涉及的金額亦可能不少。可是此類軟件需有電訊供應商配合，所以於香港並不常見。

早前曾經興起的手機通訊軟件「Line」就曾經引起類似問題。凡登記和邀請朋友使用Line都會使用短訊，用戶因此在不為意的情況下發出短訊而需額外付款。然而因為短訊是由用戶自行發出的，因此並不能算是手機保安問題。

兩、三年前Symbian手機亦有中毒個案。受感染手機會定時撥長途電話到外國，令用戶蒙受損失。這類病毒的程式開發者其實很難從中得益，但不排除有個別國家的公司基於商業考慮而發放病毒。

手機病毒事件於香港不算嚴重，但並不代表不需要防範，因為全球手機病毒問題開始流行，始終會有影響你和我的可能。

另外一個關於手機保安的常見問題就是手機遺失。現在行多人都會為手機啟用長途電話服務，用戶便可能於手機遺失至切斷服務的時段內，被人使用長途電話或漫遊數據，雖然不一定涉及個人資料，但亦會造成金錢上的損失。

至於早前荷里活明星相片外洩事件，涉及的Blackberry手機由於是一個「封閉」平台，因此由病毒引起的可能性不大。可能由於用戶未有為手機加設密碼和手機未安放好，才發生上述事件。

3. 對中小企來說，有哪些良好的智能手機資訊保安做法值得建議？

最基本的就是手機不可以隨處亂放，而且要加設密碼。這樣即使手機被人盜取或撿到都不容易使用或被盜取手機內的個人資料。另外用戶可以加裝防毒軟件加強保護。用戶還可為電郵加設密碼，加強保護，避免企業資料外洩。

因為智能手機普及，很多中小企員工都會以自己的手機查看電郵或作其他公事用途。以手機看過的電郵、文件都會儲存於手機內，令手機成為一部隨身電腦。中小企資源有限，未必有資源為企業制定政策和管理，如限制手機只可於認可地方下載軟件、手機遺失時為手機上鎖和刪除資料等。但我相信小企不久後，就會開始投放資源在手機保安上。

4. 你會向用戶或中小企提出什麼智能手機資訊保安解決方案？

市面上有一些「移動設備管理解決方案」(Mobile Device Management, MDM)可提供協助。遺失手機首先要做的不是切斷手機服務，而是遙控鎖機。當手機被鎖定後，就不能再被使用。第二步就是為手機定位，尋找它的位置。如果能找出手機，就要遙控將手機還原到原廠設定，

以防手機內的資料外洩，盡量將損失減到最低。如果用戶在海外遺失手機，只要手機仍連接網絡，香港網絡供應商亦可遙距為手機上鎖和刪除資料。而且MDM亦可定時為手機備份，這樣即使手機遺失亦不會失去所有資料。

另外就是避免到不知名的地方下載應用程式，以防手機中毒。下載程式時亦應留意可給予程式使用的權限，如果涉及重要資料就要加倍留意，同時要了解自己的責任，如果有懷疑就不要下載。更重要的是避免「越獄」。用戶亦可加裝防毒軟件，加強防護。智能手機在我們日常生活中提供不少方便，我們更應盡力保護，以手機協助我們日常工作。

我亦會建議用戶定期更新手機內的程式，如防毒程式、作業程式（Operating System, OS）等，因為現時並沒有一個作業程式完全安全。開發商會更新作業程式以防被人破解，故此更新作業程式可加強手機的保安，而且更新費用全免，更適合中小企。手機病毒有機會隨時間而增多，故此有必要經常更新防毒程式。

PCCW亦計劃為中小企和個人用戶提供行動裝置管理，以月費形式為用戶受務，希望可協助中小企以最少的資源得到最大保障。

總結

要避免由手機引起的損失，需由「個人習慣」做起。首先可留意一些有效、但免費的措施，如「機不離手」、設置手機密碼、不到不認可的地方下載程式等；第二步才是加設MDM之類的裝置，作為後備方案。改善個人習慣，是預防手機遺失和資料外洩最根本的措施。

關於PCCW mobile

PCCW mobile是香港首屈一指的電訊服務供應商「香港電訊」的業務單位之一，而香港電訊的大部分股權由電訊盈科有限公司持有。

PCCW mobile不僅提供優質話音及數據通訊，並且是電訊盈科集團獨有的「四網合一」平台之一，為各類客戶提供媒體內容及互動服務，讓用戶可按本身的生活模式，從一眾創新的流動通訊服務中挑選出切合個人所需的服務，例如實時播放的電視節目、串流數碼音樂、相片及短片分享服務、遙距監察、流動訂票、即時傳訊、電郵方案、整合式固網／流動辦公室通訊方案等。有關PCCW mobile的其他資料，請瀏覽網址：www.pccwmobile.com。

關於管紀東 (Alex Kun)

管紀東先生是電訊盈科流動通訊策略科技副總裁（無線業務），他於 1999年加入電訊盈科有限公司，在傳媒和移動行業的工作經驗超過 17年。於電訊盈科，管先生負責無線產品和服務的開發和管理，包括內容聚合，設備評估，戰略產品和服務的規劃，以及項目管理和實施。他開發了大量的移動增值服務，包括移動電視，音樂，移動定位及SMS企業解決方案，3G和Wi-Fi集成的移動寬帶服務，以及智能手機Apps等。加入電訊盈科之前，管先生於壹傳媒互動任職業務發展總監，負責互聯網業務的發展，為公司成立互聯網開發團隊，於壹傳媒他建造了超十過網站，包括收費系統和在線廣告平台。管先生自2001年以來，為香港無線科技商會會員。

受訪企業：Symantec
受訪者：林卓暉

1. 有哪些最新的智能手機資訊保安威脅值得關注？

使用智能手機或平板電腦協最大的優勢當然是方便，因為它體積小，可以隨時隨地使用；但正因為體積小，大意遺失的機會亦隨之增加。

當智能手機越來越方便時，用戶會將大量個人資料存入手機中，包括電話簿、客戶資料、電郵、報價單等敏感資料，如果這類資料落入他人手中，便有可能造成重大損失。

當你用傳統電腦時，你不會將企業的資料隨意傳給他人；但當遺失手機時，由於裏面儲存了大量企業資料，就可能發生難以估計的影響和危機。你不會知道資料會在甚麼人手上，而他又會否將資料上網公開。

智能手機的保安設計已較傳統電腦安全，但必須有用戶的充分合作。如用戶不在官方正式途徑下改動作業系統，包括「越獄」，這就會降低手機的保安設定，令手機曝露於危機之中。

手機生產商將作業系統加入限制，目的是要保護用家，因在非官方渠道下載的軟件未經生產商認証，可能被加入惡意程式，有可能會盜取手機內的資料。

另外，惡意程式可能控制手機定時傳送短訊到指定電話號碼，令用戶需付短訊費用，如果程式開發者心懷不軌，於電訊商設立「Sort Code」，當用戶手機自動傳送短訊時，開發者就可從中獲利。

總括而言，我認為智能手機的危機包括：

1. 容易遺失
2. 用戶在不完全了解的影響下，改動了手機的作業系統
3. 改動後手機出現漏洞和被裝惡意程式
4. 資料外洩

2. 可否提供一些智能手機資訊保安例子供《智能手機資訊保安實用電子指南》參考？

外國有不少有關智能手機保安問題的個案，第一個就是在智能手機上發現的間諜程式。　程式會記錄用戶發送過的SMS、曾撥出的電話、甚至記下用戶的所在位置，由於用戶毫不知情，令人防不勝防。

間諜程式一般經過第三者或以不法途徑下載到用戶的手機，例如用戶為手機「越獄」並下載未經認証的程式，而用戶根本無從知曉。通常

會發現手機電量消耗得比以前快，才揭發問題，因為間諜程式會不停傳送資料，比較耗電。

間諜程式於一般官方網站如：App Store, Android Market不會出現，只會在網上有售，大概數百元美金，但先決條件是將手機「越獄」。這亦証明為手機「越獄」等同放棄手機的安全性。

第二個問題就是用戶遺失手機。如果用戶事前沒有安裝軟件管理智能手機，遺失了手機就會完全無計可施，即使想清除手機內的檔案也不能。而且很多用戶為求方便，不會為手機加設密碼，當手機被撿後，內裡的資料如電郵等就可容易地被人查看，甚至被冒認發送電郵，騙取企業敏感資料。

第三個是關於金錢上的損失。部分惡意程式會自動、定時傳送短訊到不知名號碼，導致電話費增加。

3. 對中小企來說，有哪些良好的智能手機資訊保安做法值得建議？

第一就是要為手機加設「螢幕鎖定密碼」。設置密碼後即使手機遺失，其他人亦不能夠即時檢視手機內的資料。因此我們強烈建議用戶必須為手機上鎖，雖然會帶來少許不便，但可換來保障。

第二是不可作出系統性的改動，例如為手機「越獄」、「Root機」等。雖然改動可加強手機功能，裝置第三方的應用程式，但改動手機後，用戶便不能控制保安設定，以蘋果手機為例，App Store會為所有上架的程式認証，確保不會有惡意程式存在，但手機「越獄」等同將大門打開，令惡意程式有機會裝置到手機中。

第三是培養預防手機資料外洩的概念。根據觀察，大部分用戶都會將同時將公、私資料放置到手機中。如會將企業電郵自動轉發到私人電郵，再用手機收發。雖然相當方便，但的亦建議用戶盡量將公、私資料分開，避免混淆。

第四是企業要做好資產管理，保障企業資產。智能手機和平板電腦因流動性高，較傳統電腦方便，因此有部分中小企都會購買予員工作公事用途，但大部分企業都忽略對手機的「資產管理」。如手機是否在運作？會否有手機已經遺失？

不少企業都有計劃購置智能手機和平板電腦給員工，但其中一個阻力就是對手機管理的擔憂。因為手機派出後，公司很難監測，而且要收回又會大費周章。

第五，是在找尋手機或保安管理供應商時，必須留意供應商能否提供跨平台的服務。智能手機有各種不用的作業系統，供應商可能出現不支援某平台的問題，或令公司有額外支出。

第六，必須為手機裝置防毒程式。iPhone沒有防毒程式下載，但並非所有智能手機都不需要或沒有防毒程式，因為Android是有此類程式可供下載的。所以中小企需了解個別作業系統的特點，以訂出最適當的保安方案。

4. 你會向用戶或中小企提出什麼智能手機資訊保安解決方案？

要好好管理企業的智能手機有五個元素：
第一個就是「移動設備管理解決方案」(Mobile Device Management, MDM)，這個程式有三大主要功能：

1. 活化(Activate)。當企業購買一部全新的智能手機時，需要為手機作出多種設定，如電郵地址、無線網絡等，才可分配到員工手中。如果購買的數量較多的話就要用上較多的時間。而「活化」功能就可以自動設定，節省時間。另外亦可同一時間經系統，以非電郵形式傳送檔案到預設群組中的用戶或更新檔案。

2. 保安(Secure)。手機遺失時可透過系統清除手機內的資料，避免外洩。而且系統亦可限制手機必須設置密碼，並限制密碼長度，而且限制密碼的複雜程序，加強對手機的保護。它亦可禁止員工使用相機和螢幕截圖，以免企業敏感資料外洩。同時企業可以限制用戶下載應用程式，再進一步減低風險。

3. 管理(Manage)。首先系統可以偵測到手機有否被「越獄」，再向管理人員發出警告。而且管理人員可向該手機收回已經發出的電郵，避免企業資料經不安全的手機洩漏。

管理人員亦可知道該手機裝有的應用程式，如果違反公司規例，便可作出相對的行動。

第二個就是分隔資料的技術。有些企業已經開始進行”Bring Your Own Device”（自備裝置），以員工的私人手機同時作公事用途。但難題是如何在保障員工使用手機的同時，保護企業的資料。以一個應用程式儲存所有與工作有關的資料，方便日後管理或清除，將會是大趨勢。

第三是保安的應用程式。MDM並不包括防病毒的功能，所以用戶需了解自己正在使用的平台並實行可行的方案，以保護手機免受惡意程式攻擊。

第四是支出管理。因為跨台短訊以及漫遊數據都會令企業支出增加，所以企業亦需留意。

第五是設備與網絡的連結。如果以公司網絡傳送資料或電郵，公司可以作出監察。但當設備以電訊商的網絡發送電郵，而當中會否包含企業機密，企業就會無從知曉。因此企業亦需作出對策。

企業做到以上五個範疇，才可算是有完整的「設備管理」。

總結

中小企不應低估智能手機保安問題的潛在危險。因為手機的流動性高，可以隨時遺失，而且手機功能甚至比電腦更多。

第二是企業會開放多少手機功能予員工使用？員工必然會要求有更多功能，但管理人員能否作出相應的管理？企業應逐步推行，避免混亂，更重要的是要訂立守則，以方便管理和盡早保護當中的資料，保障企業利益。

關於Symantec

Symantec由一群有遠見的電腦科學家在 1982 年創立，並隨著科技的進步一直成長。Symantec專注為個人用戶與企業用戶提供安全、儲存及系統管理解決方案，以協助保護和管理其資訊。

關於林卓暉

林卓暉現任Symantec香港區高級系統經理，負責該公司在香港的端點保安管理及流動解決方案能配合全球業務運作。林氏作為香港的客戶解決方案及技術顧問，並在支援香港銷售團隊上扮演著關鍵的角色。

林卓暉在商業端點保安管理項目，擁有超過六年以上經驗。

林卓暉在本地資訊科技工程及產品部署具有豐富的經驗。在加入Symantec前，他曾在Asiasoft Hong Kong擔任技術經理。

林氏畢業於香港理工大學，並持有電腦工程學士學位。

受訪企業：香港電腦保安事故協調中心 (HKCERT)
受訪者：古煒德

1. 有哪些最新的智能手機資訊保安威脅值得關注？

遺失手機和處理不當是一種最常見的問題，去年每小時就有一人手機遭偷竊或遺失，在智能手機中保存的個人資料很容易會洩漏給其他人。

手機病毒 (Malware)可直接從網上感染，或在手機與電腦作同步處理時把病毒傳染給手機形成「殭屍網絡」。該應用程式本身版本並沒有問題，可以正常運作，但當它提供新版本更新時，便可能帶有一些惡意的行為，如搜集個人資料，或者控制手機等。用戶或在不知情下，從App Store把這些程式下載下來。

垃圾短信(SMS spam)由來已久，一些垃圾短訊其實是釣魚網絡（Phishing），會透過短訊中的連結，包括用一些縮短了的網址如tiny url，讓用戶登入，因而中伏。

2. 可否提供一些智能手機資訊保安例子供《智能手機資訊保安實用電子指南》參考？

有一個例子和人們頻密更換手機有關。有用戶購買了一部二手手機後，發現有些設定還未更改，剛好他和原來機主在同一間公司上班，便利用了手機原有的用戶身份及密碼，來連接上他的Wi-Fi。這個例子說明賣手機時要留意把機內的設定和內容清除，否則便可能把手機上儲存的很多資料，例如通訊記錄、電子郵箱等洩露。

此外「定位功能」(location tracking)是另一個大多數人沒有注意到的範疇。雖然目前我們沒有正式的例子去說明「定位功能」本身會構成多大的威脅，但曾經有人在facebook上公告自己什麼時間放假、到什麼地方旅行後，其住所被爆竊。因此，人們在使用「打卡」或「定位功能」的應用程式時應更加謹慎。

3. 對中小企來說，有哪些良好的智能手機資訊保安做法值得建議？

良好做法包括有「技術」和「流程」，然後要有「人」去執行。不論智能手機或傳統電腦同樣有「技術」需要，因為人手或肉眼沒有辦法

偵測自己有否中伏。此外，智能手機還多了一樣防盜功能，即在你遺失手機後可追蹤或封鎖手機，甚至刪除機內資料等。

中小企業可以安裝「移動設備管理解決方案」(Mobile Device Management, MDM) 管理智能手機，讓企業知道手機機種，如作業系統等級、安裝了什麼軟件等，企業可以拒絕登入任何未經註冊或不支援的手機。

另外企業當然要宣傳「流程」、資訊科技的措施及指引。

「人」是最薄弱的環節，因為員工始終有可能不跟從指引。

4. 你會向用戶或中小企提出什麼智能手機資訊保安解決方案？

員工用自己的智能手機上班(Bring your own device, BYOD)是最新趨勢也是一種威脅。當然企業可以安裝行動裝置管理程式，管理員工的智能手機，監管員工智能手機內可以或不可以下載什麼應用程式和文件，但手機是私人物品而不是企業提供，企業好像沒有權限指示員工應該放什麼進去，不應該放什麼，故實行有一定難度。

智能手機有助提高生產力，但它又是私人物品，在某程度上企業的資訊科技措施控制不可以太嚴厲，關鍵是怎樣在企業政策與員工信任之間取得平衡。

關於香港電腦保安事故協調中心 (HKCERT)

由香港生產力促進局管理的香港電腦保安事故協調中心，是資訊保安事故協調中心，為本地企業及互聯網用戶提供資訊保安事故的消息和防禦指引、事故回應及支援服務，及提高保安意識。

中心聯絡本地的組織，負責收集、發放訊息及協調保安事故應變行動。HKCERT 亦是全球保安事故協調中心組織 (Forum of Incident Response and Security Teams, FIRST) 及 亞太保安事故協調中心組織 (Asia Pacific Computer Emergency Responce Teams, APCERT) 的成員，與其他協調中心在跨境資訊保安事故上，交換情報和保持聯繫。

關於古煒德 (Roy Ko)

古煒德是香港生產力促進局資訊科技業發展部首席顧問，專責提供有關軟件過程改善、軟件品質保証及資訊保安的顧問服務。古先生並負責香港電腦保安事故協調中心的日常運作。

古先生是國際信息系統審計師(CISA)、特許資訊保安經理(CISM)及註冊軟件質量分析師(CSQA)，並為香港軟件過程改善專題小組(HKSPIN)創會主席及香港電腦學會資訊保安專家組秘書。

A.2 參考

歐洲網絡與信息安全局 - 智能手機：用戶的資訊保安風險，機遇和建議
http://www.enisa.europa.eu/act/it/risks-and-data-breaches/smartphones-information-security-risks-opportunities-and-recommendations-for-users

保護智能手機及平板電腦
http://www.computerlinks.hu/FMS/19183.dummies_smartphones_and_tablets_.pdf

2012年最佳智能手機保安軟件的比較和評論
http://mobile-security-software-review.toptenreviews.com

A.3智能手機安全清單

項目	是	否
機構有一個清晰，簡明的在企業內使用智能手機的保安政策。		
有指引關於甚麼資料及數據可以儲存在智能手機。		
任何未經批准的軟件或應用程序(Apps) 都不會安裝在智能手機上。		
智能手機上都有安裝防病毒及其他保安軟件。		
機構實施加密來保護智能手機的信息。		
使用智能手機傳輸專有或機密數據時，數據都經過加密。		
有指引關於使用智能手機上的Wi-Fi 及藍牙設施。		
機構安裝VPN，以監管智能手機的遙距訪問。		
用戶採取措施，以防止智能手機遺失，被竊或損壞。		
智能手機不會無人看管，任何時候都在控制範圍內。		
智能手機遺失或被竊時，員工知道如何報告事故及跟進處理。		
智能手機都做好保安設定。		
智能手機使用密碼保護。		
用戶定期備份智能手機資料，或與電腦同步作備份。		
機構對智能手機用戶進行有關智能手機保安培訓。		
機構安裝智能手機管理解決方案 (Mobile Device Management solution)		
定期檢查可用的智能手機更新，並在可能的情況下執行這些更新。		

如果答「是」的題目少於9題，企業的智能手機保安工作還有很大的改善的空間。