BYOD 安全威脅之彙整與分類

陳昱仁[1]、廖耕億[2*]、王齋諺[3]
[1,2,3]長庚大學資訊管理學系、[2]桃園長庚紀念醫院
[1]cyr@mail.cgu.edu.tw、[2]gyliao@mail.cgu.edu.tw、[3]wanggiyans@gmail.com

摘要

行動設備日益普及，自攜設備 (Bring Your Own Device, BYOD) 議題逐漸受到重視，BYOD 代表了企業行動模式的新階段，將有可能改變人們和企業未來的工作方式。在享有 BYOD 許多優勢的同時，其特性也帶來了不同以往的安全議題，而這些議題也是目前阻礙國內外企業採用 BYOD 政策之主因，因此本研究將現有的 BYOD 安全威脅和風險進行彙整與分類。本研究以現有行動安全相關組織與學者之安全威脅分類為基礎，將 BYOD 安全威脅主要分成「A.行動設備之安全威脅」、「B.企業內部之安全威脅」和「C.人員相關之安全威脅」3 大類，再對其細分 12 項子類別，共 39 項風險。

關鍵詞：自攜設備 (Bring Your Own Device)、安全威脅、分類

The Aggregation and Classification of BYOD Security Threats

Abstract

With the popularity of mobile devices, the issue of BYOD (Bring Your Own Device) becomes more and more important. BYOD stands for a new stage of enterprise mobile mode, and it will change the working ways of people and enterprises in the future. Because of the characteristics of BYOD, it not only has many advantages, but also brings some security problems which differ from the past. These security problems are also the main reason that obstructs enterprises all over the world to apply BYOD policy. Therefore, we aggregate and classify existing BYOD security threats and risks in this study. Based on the security threat classification of existing mobile security-related organizations and scholars, this study divides BYOD security threats into three categories: “A. Security threats of mobile devices”, “B. Security threats within the enterprise” and “C. Personnel-related security threats”, and then subdivides into 12 subcategories, with a total of 39 BYOD security threats aggregated by this study.

Keywords: Bring Your Own Device (BYOD), Security Threat, Classification

* 通訊作者 (Corresponding author.)

壹、前言

1.1 研究背景

諸多智慧型行動設備，如智慧型手機、平板電腦之使用已相當普及，根據 Kleiner Perkins Caufield & Byers (KPCB) 的報告指出，2012 年全球智慧型手機用戶數已上漲了十億以上[25]，人們身上開始擁有多個行動設備[18]，這些設備擁有高性能的硬體和自由軟體平台，能夠透過新一代的行動網路技術，方便且快速的連結至網際網路[16]。自行動裝置普及後，帶動企業端興起自攜設備 (Bring Your Own Device, BYOD) 之應用模式，攜帶自己行動設備以提升工作生產力。BYOD 代表了企業行動模式的新階段，有可能真正改變人們和企業未來的工作方式，然而，使用個人設備進行辦公用途，員工可以從公開環境存取敏感資料或機密資料，並且將資料保留在自己的設備，惡意軟體或惡意的網路攻擊將可能由行動設備作為媒介進入公司內部網路，將造成企業嚴重的威脅。

Courion 在 2011 年的安全調查指出，69%的企業表示所屬的員工會使用自己的行動設備連結到企業網路[2]；Check Point 在 2012 年的調查顯示約有 71%於公司的安全事件，是由行動設備所造成[16]；Juniper Networks 在 2013 年的報告中指出，所有行動平台的惡意程式由 2012 年至 2013 年 3 月增長了 614%[11];駭客與犯罪集團意識到行動設備的安全性比傳統電腦設備來得更低，作業系統以及行動應用程式更容易遭到攻擊及入侵[10]。這些行動設備大部分都缺乏了防毒軟體和防火牆的功能，儘管安裝防毒軟體，仍然有部分安全報告證明了防毒軟體對惡意程式的偵測是幾乎無效的[17]。非法行動應用程式下載管道眾多，許多惡意軟體會將現有的應用程式注入惡意程式碼，並重新包裝[26]；官方軟體發布平台也沒辦法對上傳的軟體進行全面性的審核，下載的行動應用程式便很有可能含有惡意程式[22]。根據賽門鐵克 2011 年網際網路安全威脅報告指出，於 Android 上的所有行動設備安全性威脅中，有超過一半的威脅都是在收集設備的資料或是追蹤用戶的行動[21]，當員工高度使用行動設備於公司的內部網路環境時，容易因設備本身所帶來的安全性威脅，進而造成企業資產的重大危害。

64%企業受訪者表示已遺失或是被竊取的行動設備內含有敏感的資料[15]，CPP (CPP Group Plc) 於 2011 年的調查指出，50%汰舊的設備仍然含有大量舊用戶的資料，這些行動設備儼然成了一個中央資料管理的平台，裡面擁有大量的個人資訊和敏感資訊，當這些設備離開身邊，便有資訊洩漏的潛在風險。行動設備在安全性上雖然是最被關注的問題，隱私問題卻反而被忽略，當企業為了安全性，全面監控員工設備，可能會侵害員工的隱私，要如何在安全及隱私中取得平衡，也是值得探討的議題。

1. 2 研究動機

BYOD 革命已經席捲各類企業，徹底改變我們的工作方式，根據 McAfee 和 Carnegie

Mellon University 報告指出，大約有 63%企業員工會使用行動設備處理工作事務[12]，員工不需要再使用企業所配置的行動設備，只需使用自己所擁有的設備，便可以在任何時間及任何地點對公司內部資料進行存取，企業不但可以節省設備及教育訓練之成本，員工更可以藉此提升生產力、協同作業能力和企業競爭力[2][4][8][12][15]。對企業來說，在享有 BYOD 所帶來的便利性及低成本的同時，也造成了不同以往的安全議題，因此在執行 BYOD 政策前，必須要對實體設備、網路通訊等安全性層面作全面性的考量。在現有參考文獻中，對於 BYOD 的安全性分類及評估大部分只專注於某個層面進行探討，例如：惡意程式感染途徑、行動網路的攻擊方式等[25]，然而在 BYOD 環境中，還有許多因素會使行動設備所儲存的資料遭致洩漏，需要更全面的討論。

1.3 研究目的

在實施 BYOD 政策前，確保企業機密資料的安全性和員工的隱私是最重要的議題，因此有需要全面性地了解 BYOD 環境下的安全威脅，以便於後續風險的評估和排除。本研究之目的為廣泛收集並整理現有與 BYOD 安全之相關文獻，並將各種已知的 BYOD 安全威脅和風險進行彙整與分類，期望企業管理者和企業資訊安全人員在制訂 BYOD 安全政策時可有充分之資料以供參考。

貳、文獻探討

2.1 BYOD 簡介

BYOD 是一種允許員工攜帶自己的行動設備到他們工作場所的商業政策。隨著消費性行動裝置普及，越來越多的員工希望能在其企業使用自己擁有的設備、自己的行動應用程式，並使用設備連結到企業網路，於是產生了 BYOD 的趨勢[4]。BYOD 最大好處是可以減少企業硬體採購成本，行動設備本身是員工所習慣的操作介面和系統環境，可以減少設備操作之教育訓練成本，企業允許員工在任何時間及任何地點享有企業資源的存取權，進行遠距辦公，以此大幅地促進生產力，並且增加員工的滿意程度，整體工作產能也能因行動效率而有所提升；然而在另一方面，這些行動設備也為企業開啟了資訊安全大門，讓企業的敏感資料將可能因 BYOD 政策產生更多洩漏管道，為 IT 部門帶來複雜的問題和沉重的負擔，面臨難以想像的風險[4][15][16][21]。

2.2 BYOD 風險與威脅

2012 年 RSA 大會中，有近 70%的資訊安全專家認為與其他的安全措施相比，行動

設備安全漏洞管理是非常重要的[15]。文獻[12]指出，行動安全最主要之關鍵挑戰在於如何保護敏感資料。Enterprise Strategy Group (ESG) 向 315 位在企業組織內工作的資安專業人士，對「最艱鉅的行動安全挑戰」之議題進行調查，點出了幾個主要問題，如表一所示。行動設備容易受到各類的攻擊威脅，這些威脅和攻擊簡單的總結在表二。

表一：BYOD 挑戰
（資料來源：[15]、[20]及本研究整理）

項目	說明
政策	● 行動安全政策的建立 ● 行動安全政策的落實
敏感資料	● 遺失或被竊的設備 ● 資料的機密性和完整性的保護
威脅	● 行動設備上的威脅管理

表二：行動設備常見之攻擊
（資料來源：[25]和本研究整理）

威脅和攻擊	描述
監聽 (Sniffing)	盜錄、竊聽通話內容，如：破解 GSM/A5。
垃圾訊息 (Spam)	垃圾簡訊、垃圾郵件。
欺騙攻擊 (Spoofing)	假冒的來電或是簡訊寄件者。
網路釣魚 (Phishing)	使用偽造的應用程式或網址偷取個人資訊。
網址嫁接 (Pharming)	脅持一般正常網站重新引導至惡意網站。
語音釣魚 (Vishing)	利用自動語音系統的詐騙電話。
資料洩漏 (Data Leakage)	未經授權的發送資料，如：惡意程式 ZitMo。
瀏覽器中間人攻擊 (MitB)	使用假網頁騙取登入資料。
WebKit 引擎漏洞	透過存取惡意網頁，輕易地讓手機遭到劫持。
阻斷服務攻擊 (Denial-of-Service Attack, DoS)	● 干擾 (Jamming) 無線訊號通道。 ● 簡訊的洪水攻擊 (Flooding)。 ● 電力耗盡 (Exhausting) 攻擊。

本研究整理 BYOD 研究學者對現今行動安全威脅覺得較難克服的議題，這些議題有助於風險分類和收集，分別說明如下：

- **行動設備安全性不足**：行動設備本身在設計之初並沒有嚴格的考慮到如何保護資料安全性，大多行動設備都缺乏較高的安全功能，儘管是較低的安全功能，大部分的使用者都設定成預設禁用之狀態，如：屏幕鎖定、PIN 碼鎖等[18]。
- **平台導向 (Platform-Oriented) 的行動設備**：市面上有多種的行動作業系統，如：

Android、iOS 等，安全軟體必須要可以支援不同的作業系統和版本。雖然 Android 和 iOS 目前佔行動市場手機平台的主導地位，但隨著技術的快速發展，版本不斷推陳出新，也有多個不同舊版本操作環境仍被持續使用，這創造了一個碎片化 (Fragmentation) 的問題，這使得行動設備的管理佈署變得更為困難[2][4][7][13]。

- **多入口的開放系統**：無線網路安全威脅不斷增加，藍芽或是 Wi-Fi 都有可能是潛在的惡意程式後門攻擊管道，需要擁有惡意程式的檢測、預防、刪除的功能。儘管安裝現有的防毒軟體，仍然有部分安全報告證明了防毒軟體對惡意程式的偵測是幾乎無效的[14][17][25]。
- **資料中央管理**：行動設備的安全性比傳統電腦設備來得更低，作業系統以及行動應用程式更容易遭到攻擊及入侵，行動設備裡攜帶著大量的個人資料、敏感資料等，彙整了大量的使用者資訊，使行動設備容易成為被攻擊的目標[10][15]。
- **資源受限的設備**：行動設備沒有如桌上電腦般擁有強大的運算能力，安全解決方案必須要考慮到計算的複雜性和電池的消耗[25]。
- **嵌入式感測器 (Embedded Sensors) 應用**：GPS、陀螺儀等感測裝置會記錄使用者的個人資訊，有被竊取或濫用的風險，相機、錄音器之功能容易將公司敏感訊息記錄並流出，應該要監控和智能化的阻止感測器未授權的存取[4][25]。
- **設備遺失和受竊**：當員工行動設備遺失，設備可能導致企業內部的訊息被竊取，即使設備不包含機密資料，仍然可從應用程式或快取憑證輕易的滲透至企業網路中，員工如果離職，儲存在設備內的企業資料將是重大的威脅，這些資料可能會移轉至競爭對手之中[4][14][15][18][23]。
- **使用者缺乏安全意識**：使用者本身對資訊安全的觀念較不重視，設定的密碼強度相當貧弱，習慣使用第三方軟體平台下載非法程式，設備本身不願更新韌體或是安全套件等，需要進行資安觀念再教育和安全政策雙向同步實行[18][22]。
- **個人與公司資料的混合**：個人的資料的隱私內容很有可能不慎至企業伺服器中，其資料更可能包含惡意程式，由行動設備移轉到公司內部網路，將蔓延至商業文件，嚴重影響整個企業的資產[18]。需有效地在同一台設備上隔離兩個空間，分別使用於個人和業務兩種用途[2][4][20][25]。
- **公有雲應用程式**：為了讓使用者所有設備擁有所需要的同一份文件，員工在工作環境中常使用一個或多個雲端共享程式，這樣的雲端服務起初是為了一般使用者所設計的，其缺乏集中控制和監控的功能，惡意程式會因同步的方式傳送到多台行動設備，機密資料也容易因雲端共享程式移轉出設備及企業內部網路。許多雲端供應商聲稱其擁有資料之使用權及控制權，這將對公司帶來敏感資料洩漏的風險，往往也不受企業所信任[15][18]。
- **解決方案建置於私有雲**：在企業內部的資料中心運行雲端服務，可提供雲端技術的可擴展性和成本效益之優點，減少了在公有雲上的安全性及可用性之威脅，企業應將解決方案佈署在私有雲上，使 IT 部門能夠控制資料位置和資料的可用性[18]。

- **惡意程式與殭屍網路威脅**：行動威脅主要可以分成幾類，如惡意程式、間諜軟體、惡意程式、OTA 攻擊 (Over The Air Attacks)、阻斷服務攻擊以及行動殭屍網路 (Mobile Botnets, MoBots)[6]，這些針對行動設備之攻擊有逐年提升的趨勢，通常會偽裝成正常軟體，讓使用者下載到行動設備，由於行動設備儲存了大量個人資訊，容易吸引惡意攻擊者的注意，增加敏感資料洩漏之可能性[15][18][25]。
- **惡意程式偵測技術**：行動安全應用程式如同一般電腦所使用的防毒軟體，目前僅只有 Google Play、Blackberry's App World、Nokia's Store 三處下載市集有提供行動安全應用程式之下載，App Store、Windows Phone 市集尚未提供。儘管如此，有相關行動安全調查指出現有的行動惡意程式偵測技術效果相當有限[22]。
- **行動網頁瀏覽器**：網頁瀏覽器本身會包含瀏覽記錄、Cookie、存取憑證、帳號密碼之暫存等，即使設備的防毒軟體已經是最新版本，也容易遭到惡意攻擊者竊取資訊，例如：瀏覽器中間人攻擊 (Man in the Browser, MitB)，IT 人員也較難控制使用者所選用的瀏覽器以及其版本、安全更新、外掛 (Plug-ins)等[15]。
- **軟體下載平台審核機制**：行動應用程式大多是透過官方交易市場進行下載，其做為中央下載點之特性，非常適合佈署惡意程式偵測程式。Google Play 及 App Store 對軟體之審核過程及偵測機制不透明且不足，且並未能確保從官方下載的應用程式便絕對安全[22]。
- **服務安全威脅**：行動設備會使用一些行動服務，例如導航服務、基於位址的廣告服務，或是行動醫療照護、行動網路銀行、社群網路服務，其服務包含之資訊都可能遭受惡意攻擊者盜取及濫用[16]。
- **法律體制威脅**：法律制度是一個不確定性高的議題，行動設備本身是由 PC 和通訊設備結合而成的個體，目前的法律無法與時俱進持續更新條款，法律責任上難以釐清及歸咎責任[16][20]。
- **資料明文儲存**：行動設備較不著重各別資料的保護，大部分都以明文的方式進行儲存，需仰賴額外的安全程式對行動設備進行保護[16][23] [25]。
- **資料存取**：員工離職後，IT 部門若沒即時刪除員工存取企業資源的權限，離職員工便可輕易進入企業內部網路存取資料，將嚴重危及企業敏感資料的安全性。當使用者試圖存取資料時，需要經過行動簡訊 (Short Message Service, SMS)、令牌 (Token)、憑證 (Certificate)、智慧卡 (Smart Card)等多重驗證機制授權，以杜絕非法使用者或未授權者對資料進行存取[20][25]。
- **員工隱私**：BYOD 的廣泛應用使得企業組織為了達到較高的安全性，會對行動設備進一步進行資料探勘，員工的個人設備存放著許多私密資訊，這將嚴重侵犯員工隱私，心理層面會受到強烈的抵觸[6][14][20][25]。

參、BYOD 安全威脅分類

本研究以現有行動安全相關組織與學者之安全威脅分類為基礎，將 BYOD 安全威脅主要分成「A.行動設備之安全威脅」、「B.企業內部之安全威脅」和「C.人員相關之安全威脅」3 大類，再對其細分 12 項子類別，共 39 項風險，如表三、表四和表五所示，分別說明如下。

表三：BYOD 安全威脅分類－－A.行動設備之安全威脅

子類別	安全威脅（風險）
A.1 資料安全	A.1.1 資料儲存未加密 A.1.2 個人資料中央管理 A.1.3 行動設備加密方式不安全
A.2 作業系統安全	A.2.1 Android 作業系統版本碎片化程度高 A.2.2 作業系統安全強度不一致 A.2.3 系統組態設定不安全 A.2.4 未對系統進行安全性更新 A.2.5 超級使用者權限造成系統威脅
A.3 硬體設備	A.3.1 安全數位記憶卡 (Secure Digital Memory Card) 無法加密 A.3.2 受限硬體計算能力 A.3.3 設備周邊功能被濫用 A.3.4 設備遭竊或遺失
A.4 應用程式安全	A.4.1 應用程式不合理的權限存取 A.4.2 未更新應用程式 A.4.3 應用程式供應平台審核機制薄弱 A.4.4 應用程式易被注入惡意碼 A.4.5 收集感測應用程式 (Sensory Applications) 之數據 A.4.6 不受信任的公有雲應用程式 A.4.7 行動網頁瀏覽器易遭受攻擊
A.5 通訊及網路安全	A.5.1 行動網路釣魚 A.5.2 阻斷服務攻擊 A.5.3 行動殭屍網路

A. 行動設備之安全威脅

A.1 資料安全

A.1.1 資料儲存未加密

通過資料加密來保護數位資產，是防止未經授權洩漏重要手段，行動設備可能會攜

帶企業敏感資料，這些資料不該在行動設備中以明文的方式儲存，也因原生行動設備較不著重各別資料的保護，需仰賴額外的安全程式對行動設備進行保護[16][23][25]。

A.1.2 個人資料中央管理

行動設備裡攜帶著大量的個人資料，如通訊錄、備忘錄、行事曆、瀏覽器記錄或應用程式夾帶的資訊，行動設備彙整了大量的使用者資訊，使行動設備容易成為被攻擊的目標[10][19][25]。

A.1.3 行動設備加密方式不安全

現有加密機制與演算法因密碼分析和破譯方法的進步，使得許多加密方式不完全安全，也因行動設備受限於運算能力無法迅速加解密高複雜度的演算法，使得行動設備資料的機密性產生了疑慮[25]。

A.2 作業系統安全

A.2.1 Android 作業系統版本碎片化程度高

Android 和 iOS 目前佔行動市場手機平台的主導地位，但隨著技術的快速發展，也有多個不同舊版本操作環境仍被使用著，這些舊版本的安全漏洞仍然存在著，甚至也不再進行安全性更新，這創造了一個碎片化 (Fragmentation) 的問題，這使得行動設備的管理佈署變得更為困難[2][4][7][25]。

A.2.2 作業系統安全強度不一致

BlackBerry 以及 iOS 為非開性放平台，並且支援多重的軟硬體安全機制，相較於 Android 威脅性較低，相反的 Android 為市佔率高的開放性作業平台，容易成為惡意攻擊者的目標，且大部分操作權限都掌控在使用者手中，自由度高卻也容易面臨安全威脅[1][4][15][25]。

A.2.3 系統組態設定不安全

作業系統之弱點常來自於組態設定的缺失，現有的行動作業系統會有原生自帶的安全性功能，例如：PIN 碼、iOS Find-My-iPhone，使用者往往會貪圖方便或不清楚功能而未進行設定[18][23]。

A.2.4 未對系統進行安全性更新

行動設備使用者未定期更新用以修補作業系統漏洞的韌體，使駭客或惡意程式更容易對行動設備的敏感資料造成威脅[25]。

A.2.5 超級使用者權限造成系統威脅

越獄 (Jailbreak, JB) 或 Root 強制取得超級使用者 (Super User) 權限的方式，受到沙盒保護的行動應用程式將能被任意讀取，並且破壞系統本身的安全性，容易遭受到攻擊者的惡意行為以及感染惡意程式[5][22]。

A.3 硬體設備

A.3.1 安全數位記憶卡 (Secure Digital Memory Card) 無法加密

行動設備儲存方式除了內建的 ROM 外，普遍還是使用 SD 卡擴充儲存量，除了 iOS 本身不支援擴增 SD 卡外，其他平台皆支援此功能，SD 卡未加密將可能因 SD 的移轉同時將敏感資訊外洩[1]。

A.3.2 受限硬體計算能力

行動設備現今還無法取代 PC 的運算速度，一般在 PC 能使用的防毒軟體或是安全解決方案，於行動設備上並未能完全套用，其功能也大受到限制[25]。

A.3.3 設備周邊功能被濫用

相機以及錄音功能是現今行動設備的基本配備，內部惡意員工可利用此功能將公司敏感訊息記錄並流出，惡意攻擊者有可能遠端遙控員工行動設備啟用這些功能，應該要監控和智能化的阻止相機或錄音程式未授權的啟用[4][25]。

A.3.4 設備遭竊或遺失

當員工行動設備遺失或被竊，可能導致企業內部的訊息被竊取，甚至落入競爭者手中，即使設備不包含機密資料，仍然可從應用程式或快取憑證輕易的滲透至企業網路，將對企業造成嚴重威脅[4][5][12][13][15]。

A.4 應用程式安全

A.4.1 應用程式不合理的權限存取

Android 應用程式安裝前會要求開放存取權限，例如：聯絡資料、硬體控制、相片多媒體檔案等，大部分使用者毫不猶豫接受權限開放，卻沒細看開放了哪些項目，這將使行動設備敏感資料暴露在風險之中[1][15]。

A.4.2 未更新應用程式

應用程式的更新除了是推出新功能外，更常是為了填補應用程式上的漏洞，若未即時進行更新，將使駭客或惡意程式更容易對行動設備的敏感資料造成威脅[18][25]。

A.4.3 應用程式供應平台審核機制薄弱

行動應用程式下載市集對惡意程式的審核機制薄弱，實際的審核機制並不透明且未進行完整性檢查，即使從官方市集所下載的軟體，都可能含有惡意程式[22]。

A.4.4 應用程式易被注入惡意碼

Android 作業系統的開放和自由性，將吸引惡意攻擊者的目光，能透過將惡意程式偽裝成主流程式，甚至將正規程式其植入惡意碼，散播在網路上供人下載，進一步收集行動設備上的敏感訊息[5][21][22][26]。

A.4.5 收集感測應用程式 (Sensory Applications) 之數據

感測應用程式包括 GPS、陀螺儀、加速度感測器等，這些程式將會記錄使用者的行為模式，能夠追蹤及預測使用者的行為，使用者的個人資訊，有被竊取或濫用的風險[4]。

A.4.6 不受信任的公有雲應用程式

為了讓所有設備都有自己所需要的文件，人們常使用一個或多個雲端共享程式，惡意程式會因同步的方式傳送到多台行動設備，機密資料也容易因雲端共享程式移轉出設

備及企業內部網路，雲端供應商擁有資料之使用權及控制權，這將對公司帶來敏感資料洩漏的風險，往往也不受企業所信任[14][18][19]。

A.4.7 行動網頁瀏覽器易遭受攻擊

網頁瀏覽器本身會包含瀏覽記錄、Cookie、存取憑證、帳號密碼之暫存等，即使設備的防毒軟體已經是最新版本，也容易遭到惡意攻擊者竊取資訊，例如：瀏覽器中間人攻擊 (Man in the Browser, MitB)，IT 人員也較難控制使用者所選用的瀏覽器以及其版本、安全更新、外掛 (Plug-ins) 等[15]。

A.5 通訊及網路安全

A.5.1 行動網路釣魚

惡意攻擊者可能會設定一個無需密碼的公共 Wi-Fi 存取點進行釣魚，使用者貪圖方便連結使用後，其傳輸資料之內容將可能被監聽甚至遭竊取；行動應用程式釣魚或網站釣魚皆能將使用者導向至惡意的網頁，威脅行動設備資料安全[25]。

A.5.2 阻斷服務攻擊

惡意攻擊者能透過一些方式攻擊達到阻斷服務的效果，例如：頻道的干擾將無法使用網路服務；簡訊洪水攻擊能使簡訊儲存空間占滿，無法使用簡訊服務；惡意程式會於系統後台持續執行動作，增加電量迅速耗損，最終因電量耗盡無法使用行動設備[25]。

A.5.3 行動殭屍網路

殭屍電腦攻擊者 (Botmasters) 已經開始針對行動設備及網路，因為這些行動設備相較於一般的電腦而言往往沒有適當的安全保護，受到感染的行動設備將可能受到行動銀行攻擊 (Mobile Banking Attack)、竊取個人資料、非法傳輸資訊、下載惡意程式以及更改設備的組態設定等[6]。

表四：BYOD 安全威脅分類－－B.企業內部之安全威脅

子類別	安全威脅（風險）
B.1 資料混合	B.1.1 個人與企業資料未隔離
B.2 政策執行	B.2.1 政策部署困難 B.2.2 未持續更新安全政策 B.2.3 未對設備進行追蹤監控
B.3 加密	B.3.1 資料傳輸未加密 B.3.2 資料本身未加密 B.3.3 加密演算法安全性不足
B.4 身分存取管理	B.4.1 未即時刪除離職員工存取權限 B.4.2 身分授權檢查不足

B. 企業內部之安全威脅

B.1 資料混合

B.1.1 個人與企業資料未隔離

個人文件可能包含惡意程式，經由行動設備移轉到公司伺服器，將會蔓延至商業文件，嚴重影響整個企業的資產，空間隔離能在行動設備上隔離個人和組織的空間，使得不同的安全策略可以被應用[2][4][20][25]。

B.2 政策執行

B.2.1 政策部署困難

行動設備作業系統、版本碎片化程度高，導致 IT 人員難以對行動設備進行控管。過度管理將侵犯員工的隱私，最低限度的管理將造成企業敏感資料洩漏的風險[2][14][18][20][25]。

B.2.2 未持續更新安全政策

行動硬體設備的普及，許多針對行動設備的各型態惡意攻擊如雨後春筍般持續增長，企安全政策須不斷更新，以符合最適的安全需求及應付新的安全威脅[2][15]。

B.2.3 未對設備進行追蹤監控

追蹤監控對企業組織來說，是非常重要的功能，透過監控可在資料洩漏前檢測出異常行為，有效追蹤惡意員工的設備位置和查閱操作記錄，保護公司機密訊息的安全[14][25]。

B.3 加密

B.3.1 資料傳輸未加密

企業內部對內部以及外部對內部的資料傳輸如果未使用加密功能，將造成資料洩漏，例如：竊聽網路、偷取使用者 Cookie、盜用憑證，內部攻擊者可能藉此取得敏感資料或權限憑證進行資料竄改，外部攻擊者也可藉此輕易地進入企業內部網路[15][20]。

B.3.2 資料本身未加密

企業急需首要探討的是如何保護敏感資料不外洩，其最重要的便是保護資料本身，資料加密可確保當資料不幸被惡意攻擊者取得或移轉時，可以更進一步保護資料的安全，減少機密洩漏的風險[16][25]。

B.3.3 加密演算法安全性不足

現有加密機制與演算法因密碼分析和破譯方法的進步，使得許多加密方式不完全安全，企業資料中心儲存的資料其完整性與機密性也因此出現疑慮[25]。資料經由資料中心至行動設備端的傳輸過程也需要透過安全的加密方式保護，例如：SSL 和 TLS 加密等，但有許多文獻指出其加密方式並不絕對安全[15][27]。

B.4 身分存取管理

B.4.1 未即時刪除離職員工存取權限

員工離職後，IT 部門若沒即時刪除員工存取企業資源的權限，離職員工便可輕易進入企業內部網路存取資料，將嚴重危及企業敏感資料的安全性[25]。

B.4.2 身分授權檢查不足

授權檢查不足會導致員工可以在非授權的情況下瀏覽或是存取非權限範圍的資料，需避免企業內部或外部未經授權的非法存取[20][25]。

表五：BYOD 安全威脅分類－－C.人員相關之安全威脅

子類別	安全威脅（風險）
C.1 安全意識	C.1.1 未對設備設定安全防護 C.1.2 經由第三方下載平台安裝應用程式 C.1.3 舊設備資料未完全移除 C.1.4 未即時進行安全性更新
C.2 隱私	C.2.1 設備被完全監控 C.2.2 濫用 GPS 掌握員工行蹤 C.2.3 未經同意讀取設備資料
C.3 法律	C.3.1 資訊保護模糊地帶

C. 人員相關之安全威脅

C.1 安全意識

C.1.1 未對設備設定安全防護

大部分使用者因為使用習慣或是便利性，將設備原生所提供的基本的安全功能設定成默認禁用之狀態，例如：螢幕鎖定、登入 PIN 碼等，這將設備暴露於風險之中[18]。

C.1.2 經由第三方下載平台安裝應用程式

使用者常因貪小便宜，不願支付行動付費軟體之費用，選擇從第三方下載平台下載非法軟體，這些軟體往往都夾帶著木馬或是惡意程式，竊取行動設備上的資訊[18][22]。

C.1.3 舊設備資料未完全移除

行動設備汰換率非常高，使用者大部分汰換下的行動設備皆轉售予其他買家，舊設備資料若無完整移除，設備所儲存的個人資訊及企業資料將可能轉交他人之手[24]。

C.1.4 未即時進行安全性更新

系統、應用程式之版本更新，除了推出新功能外，大多是為了修補程式漏洞，使用者若未對軟體進行更新，程式漏洞將可能造成資訊安全上的風險[18][22]。

C.2 隱私

C.2.1 設備被完全監控

企業組織為了達到較高的安全性，會選擇對行動設備進行完全監控的政策，員工的行動設備將毫無隱私可言，心理層面會受到強烈的牴觸[6][14][20][25]。

C.2.2 濫用 GPS 掌握員工行蹤

GPS 定位功能在手機遺失進行追蹤，現今行動設備遺失解決方案便會利用此方式尋找設備的具體位置，若企業掌控了員工行動設備的定位功能及其資訊，將可知道員工的所有行蹤，嚴重侵犯隱私[20][25]。

C.2.3 未經同意讀取設備資料

行動設備為私人設備，其儲存企業資料外還存有許多私人隱密資料，倘若沒清楚界定或隔離，現有安全性較高的解決方案將能查看設備中所有資訊、文件、檔案、影音，其內容將一覽無遺，員工隱私將受到嚴重的威脅[14][20][25]。

C.3 法律

C.3.1 資訊保護模糊地帶

法律制度是一個不確定性高的議題，行動設備本身是由 PC 和通訊設備結合而成的個體，目前的法律無法與時俱進持續更新條款，法律責任上難以釐清及歸咎責任[6][16][19][20]。

肆、結論與未來方向

本研究為廣泛了解現在 BYOD 安全威脅，蒐集國內外資訊安全組織之調查報告、防毒軟體公司與 BYOD 議題相關之白皮書，BYOD 現在解決方案以及學者的研究論文，另外也不斷蒐集 BYOD 安全威脅相關之資料，盡可能彙整此領域相關專家學者所討論之安全威脅。廣泛閱讀並整理現有文獻後，本研究將現有 BYOD 安全相關文獻提出之 BYOD 安全威脅進行彙整，將安全威脅形式區分為「行動設備之安全威脅」、「企業內部之安全威脅」以及「人員相關之安全威脅」3 大類，其中行動設備之安全威脅又可細分成 5 小類，企業內部之安全威脅又可細分 4 小類，人員相關之安全威脅又可細分 3 小類，共 12 小類、39 項安全威脅。

本研究針對 BYOD 之安全威脅進行彙整與分類，期望能盡可能涵蓋 BYOD 環境下所有的資訊安全威脅，但難免會有些文獻蒐集上疏漏，以致不夠全面，在後續研究中應持續收集相關文獻。另外，除了安全威脅之分類外，如何識別這些安全威脅、如何評估安全風險，以及如何部署安全解決方案等，都還需要再繼續深入研究。

參考文獻

[1] S. Adibi, “Comparative Mobile Platforms Security Solutions,” *2014 IEEE 27th Canadian Conference of Electrical and Computer Engineering (CCECE)*, pp. 1-6, 2014.

[2] J. M. Chang, P. C. Ho and T. C. Chang, “Securing BYOD,” *IEEE IT Professional*, Vol. 16, No. 5, pp. 9-11, 2014.

[3] Cloud Security Alliance (CSA), “Security Guidance for Critical Areas of Focus in Cloud Computing V2.1,” https://cloudsecurityalliance.org/csaguide.pdf, December 2009.

[4] J. H. Ding, R. Chien, S. H. Hung, Y. L. Lin, C. Y. Kuo, C. H. Hsu and Y. C. Chung, “A Framework of Cloud-based Virtual Phones for Secure Intelligent Information Management,” *International Journal of Information Management*, Vol. 34, No. 3, pp. 329-335, 2014.

[5] EC-Council, “Module 15. Hacking Mobile Platforms,” *Ethical Hacking and Countermeasures*, Certified Ethical Hacker version 9 (CEHv9) Exam 312-50, 2016.

[6] M. Eslahi, M. V. Naseri, H. Hashim, N. M. Tahir and E. H. M. Saad, “BYOD: Current State and Security Challenges,” *IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, pp. 189-192, 2014.

[7] D. Han, C. Zhang , X. Fan, A. Hindle, K. Wong and E. Stroulia, “Understanding Android Fragmentation with Topic Analysis of Vendor-Specific Bugs,” *2012 19th IEEE Working Conference on Reverse Engineering (WCRE)*, pp. 83-92, 2012.

[8] K. Hess, “How to Evaluate Mobile Management Solutions,” *Tom's IT PRO*, http://www.tomsitpro.com/articles/evaluating-mobile-management-solutions,2-708-2.html, March 2014.

[9] M. John, "Information Systems Security: A Comprehensive Model," *Proceedings of the 14th National Computer Security Conference*, 1991.

[10] Juniper Networks Mobile Threat Center (MTC), “2011 Mobile Threats Report,” http://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2011-mobile-threats-report.pdf, February 2012.

[11] Juniper Networks Mobile Threat Center (MTC), “Juniper Networks Third Annual Mobile Threats Report: March 2012 through March 2013,” https://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2012-mobile-threats-report.pdf, June 2013.

[12] K. J. Kim and S. P. Hong, “Study on Enhancing Vulnerability Evaluations for BYOD Security,” *International Journal of Security and Its Applications*, Vol. 8, No. 4, pp. 229-238, 2014.

[13] Microsoft TechNet Library, “MDM System Overview,” http://technet.microsoft.com-

/en-us/library/cc135589(TechNet.10).aspx, October 2008.

[14] K. W. Miller, J. Voas and G. F. Hurlburt, "BYOD: Security and Privacy Considerations," *IT Professional*, Vol. 14, No. 5, pp. 53-55, 2012.

[15] B. Morrow, "BYOD Security Challenges: Control and Protect your Most Sensitive Data," *Network Security*, Vol. 2012, No. 12, pp. 5-8, 2012.

[16] W. H. Park, D. H. Kim, M. S. Kim and N. Park, "A Study on Trend and Detection Technology for Cyber Threats in Mobile Environment," *2013 International Conference on IT Convergence and Security (ICITCS)*, pp. 1-4, 2013.

[17] H. Pilz and S. Schindler, "Are Free Android Virus Scanners Any Good," *AV-TEST Report*, 2011.

[18] H. Romer, "Best Practices for BYOD Security," *Computer Fraud & Security*, Vol. 2014, No. 1, pp. 13-15, 2014.

[19] V. Samaras, S. Daskapan, R. Ahmad and S. K. Ray, "An Enterprise Security Architecture for Accessing SaaS Cloud Services with BYOD," *Australasian Telecommunication Networks and Applications Conference*, pp. 129-134, 2015.

[20] A. Scarfo, "New Security Perspectives around BYOD," *Proceedings of the 2012 7th International Conference on Broadband, Wireless Computing, Communication and Applications*, pp. 446-451, 2012.

[21] Symantec, "2011 Internet Security Threat Report," http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf, April 2012.

[22] D. Titze, P. Stephanow and J. Schutte, "A Configurable and Extensible Security Service Architecture for Smartphones," *2013 27th International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, pp. 1056-1062, 2013.

[23] D. W. K. Tse, "A New Smartphone Privacy Protection Scheme based on Anti-theft Technology," *Computer Audit Association*, No. 30 ,2014

[24] P. Wagenseil, "Half of Used Cellphones Still Hold Personal Data," *NBC News*, 2011.

[25] Y. Wang, J. Wei and K. Vangury, "Bring Your Own Device Security issues and challenges," *2014 IEEE 11th Consumer Communications and Networking Conference (CCNC)*, pp. 80-85, 2014.

[26] Y. Zhou and X. Jiang, "Dissecting Android Malware: Characterization and Evolution," *2012 IEEE Symposium on Security and Privacy (SP2012)*, pp.95-109, 2012.

[27] IThome，「TLS 加密協定竟然也不安全！企業須審慎內部漏洞」，http://www.ithome.com.tw/promotion/93094，民國 103 年。