白皮書

網路安全門戶洞開

研究顯示印表機對數位攻擊的防禦能力非常低落

IT 團隊只顧著保護其他端點，公司的印表機安全卻遲滯在後

印表機是容易被有心人士鎖定的攻擊目標：許多連接網路的印表機都沒有存取限制，也沒有受到安全鎖定。

但真實世界中的威脅步步逼近，保護措施刻不容緩。企業級的印表機不斷升級，成為功能強大的聯網裝置，但仍和網路上的其他端點一樣，有著許多有機可乘的漏洞。這些端點通常都不會受到妥善保護，無異於對網路攻擊者門戶洞開，讓他們有機可乘。這樣的漏洞將公司的財務與隱私資料置於莫大風險之中，可能對公司造成難以彌補的嚴重後果。

即便如此，Spiceworks 公司最近針對 300 多位在業界擔任管理要職的 IT 人員進行調查訪問，結果顯示，僅 16% 的受訪者認為印表機可能處於安全性威脅/入侵的極高風險之中，與桌上型/筆記型電腦和行動裝置的可能承受的安全風險比例相比還要低得多。[1] 這樣錯誤的看法，導致 IT 人員將網路暴露於安全性風險之中而不自知。雖然有近六成的公司會針對印表機實施安全性作法，這樣的比例卻遠不及對於其他端點所付出的心力，使印表機成為讓某些不法分子有機可乘的漏洞，然而保護此輸入端點的解決方法，其實相當輕鬆簡單。

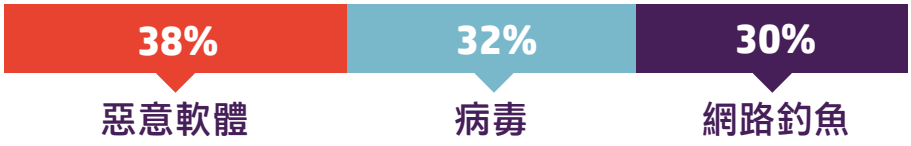
本白皮書將根據 Spiceworks 的調查研究，列出印表機安全性的相關資料，以及近期所推出的印表機內建專為防範數位攻擊的安全性功能。

僅 16% 的受訪者認為印表機可能處於安全性威脅/入侵的極高風險之中。[1]

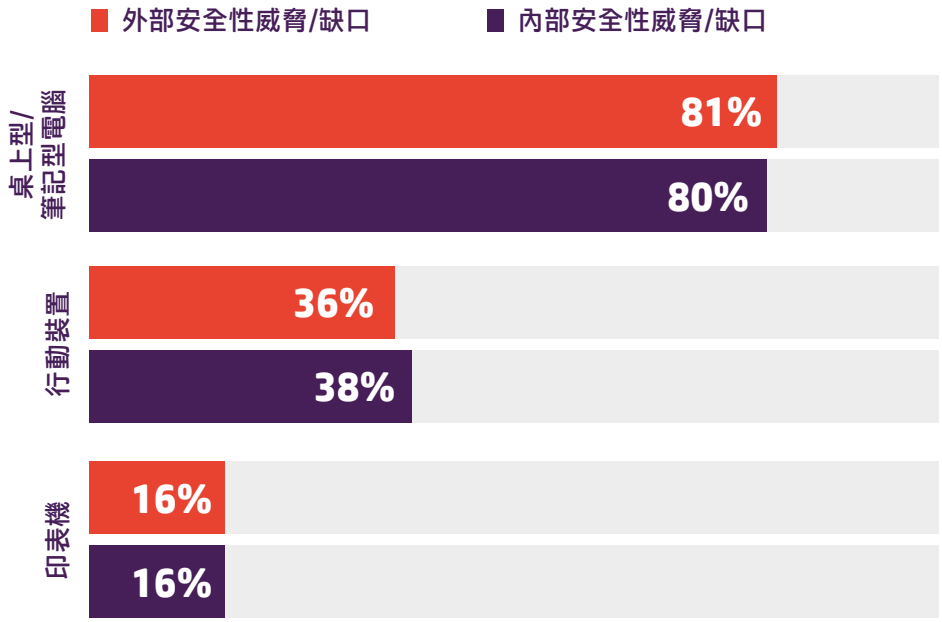
攻擊門戶大開

根據 Spiceworks 的調查研究，74% 的受訪者（實際受訪者）表示他們公司在過去一年中，曾經遭受至少一次的外部 IT 安全性威脅或入侵。而 70% 的受訪者（實際受訪者）則親身體驗過內部 IT 安全性威脅或入侵，最常見的是使用者錯誤、以個人裝置進行工作業務，或者員工使用家用或公共網路進行工作業務。[1]

最常見的 IT 安全性威脅/入侵



最常見的威脅主要從桌上型電腦和筆記型電腦潛入，其他威脅則透過行動裝置和印表機而來。[1]（根據 Spiceworks 研究，有 16% 的威脅是經由印表機而來，此數據比 2014 年的 4% 高出許多。）電腦和行動裝置經常密切監測，而印表機往往受到冷落，也可能是此原因，造成人們低估經由印表機發動的網路攻擊之數量。



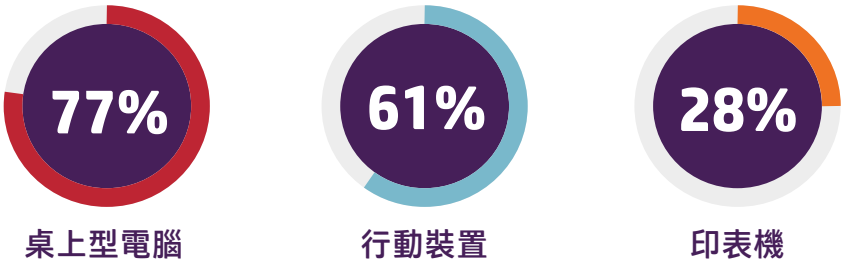
對印表機的關注程度嚴重不足

無論數據情況為何，Spiceworks 的調查也彰顯了一點——人們往往在事件發生後，才會回過頭來檢討印表機的安全性。

公司總是積極投身防範網路、端點和資料安全性。事實上，超過四分之三的受訪者都會運用網路安全性、存取控制/管理、資料保護功能，或者端點安全性——少則擇一運用，多則結合使用。[1]

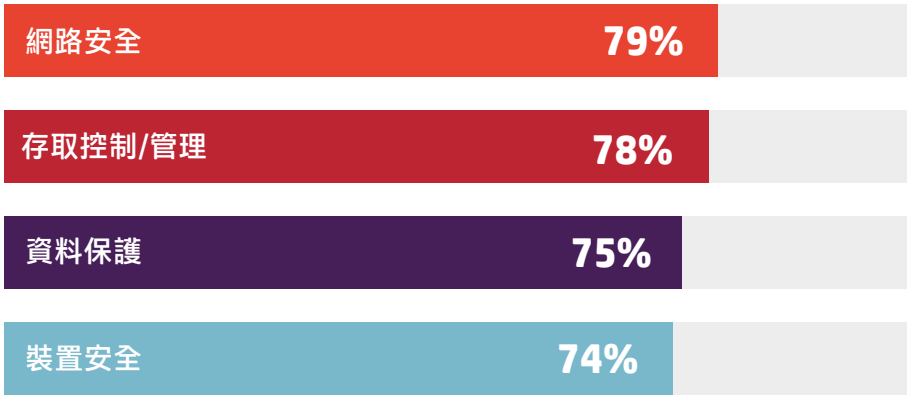
但是，這些安全性解決方案鮮少部署於印表機上。83% 的受訪者在桌上型/筆記型電腦上使用網路安全性功能，55% 的受訪者會在行動裝置上使用網路安全性功能，卻只有 41% 的受訪者會在印表機上部署相同功能。[1]

此般差異在端點安全性上顯得更加懸殊：



此外，僅不到三分之一的受訪者會於印表機部署安全性憑證，相較之下 79% 的受訪者會於桌上型電腦加以部署，54% 的受訪者會於行動裝置加以部署。[1]

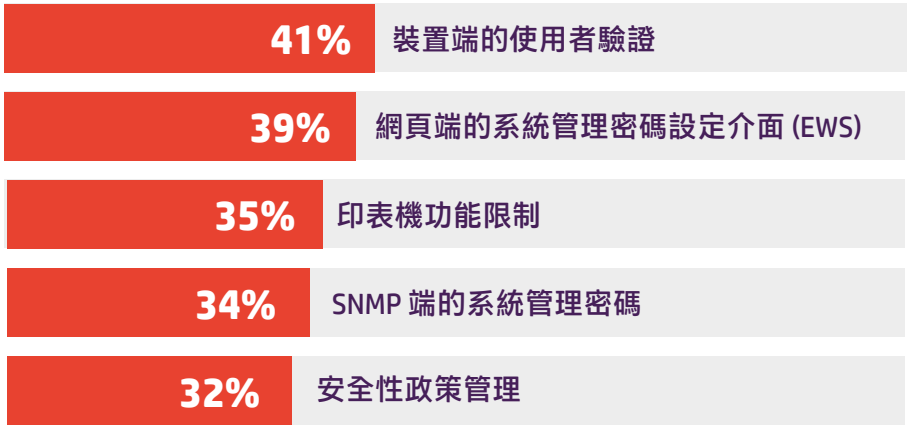
端點安全性最佳作法



用於大部分端點裝置的保護措施中，最常使用於印表機的安全型舉措為文件安全性、網路安全性和存取控制功能，但僅不到一半的受訪者表示任職之公司於印表機上使用任一舉措。[1]

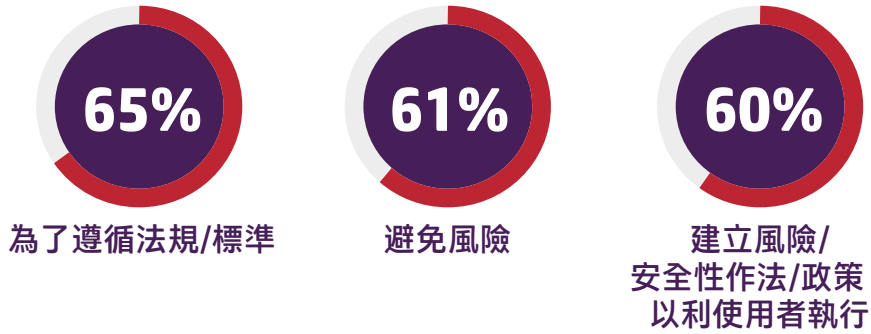
有些公司的確針對印表機實行特定的安全性作法，但即便如此，這些做法也迥然相異。僅 40% 以上的組織會部署使用者驗證功能，且不到 40% 的公司曾在網頁設定介面中使用系統管理員密碼。[1] 為了確保印表機安全無虞，所有公司都應該至少混合採用此些方法，而且防範的做法永不嫌多。

針對印表機的最佳資安法則



對於端點的法規遵循和稽核作法，印表機的安全控制功能往往比其他端點要落後得多。近 90% 的組織都部署了資訊安全政策，但這些政策往往不會惠及印表機。舉例來說，57% 的受訪者表示他們在桌上型電腦上部署了惡意軟體保護功能，但僅 17% 的受訪者將之部署於印表機上。[1]

近九成的 IT 專業人士表示，任職的公司
已經完成資訊安全政策部署到位的原因如下：



公司顯然沒有以足夠認真的態度對待印表機安全性，但此問題絕對不容小覷。

HP 首席安全顧問 Michael Howard 於六月份告訴 Computerworld：「許多印表機仍沿用預設密碼，或者連密碼這道防線也付之闕如，再或者就是有十個人使用同一密碼的情形。不受密碼保護的印表機，對駭客而言就像是取之不絕的金山寶礦。我們常見的入侵事件，通常是「從中搞鬼」式的攻擊——他們會取得印表機的控制權，並將待列印文件在付諸紙本前轉移至另一台筆記型電腦。如此一來，他們就能對 CEO 列印的文件一覽無疑。」[2]

列印人員遭受入侵的潛在影響

根據 Bitdefender 的資深數位威脅分析師 Bogdan Botezatu 表示，印表機代表著規模相當大的潛在安全性漏洞。「我們的安全漏洞評估實驗室中，接到了大量遙測資料。路由器已經不再是網路中最容易遭受攻擊的裝置。現在已由印表機取而代之。」[3]

這樣的漏洞可能對業務造成難以彌補的巨大衝擊。只要有一台印表機未受妥善安全保護，就無異於將所有聯網裝置暴露於攻擊的風險之中，讓駭客有機可乘，進一步窺視聯網裝置，對整個網路的安全性造成莫大損害。

1. 服務台電話與支援時間增加

2. 生產力與效率降低

3. 系統停機時間增加

4. 支援電話時長增加

5. 使用者政策加強執行

我們都深知安全性入侵會帶來的負面影響。在 Spiceworks 的調查中，受訪者表示受到入侵的頭五大影響如下：[1]

如果印表機遭到入侵，後果將更為嚴重，尤其是您若使用能夠以電子方式儲存已列印資料的多功能印表機時，更是不堪設想。將已列印的內容儲存在印表機的緩存中，讓駭客有機可乘，獲得個人或商業的機密資訊。

更讓人感到擔憂的是，駭客可以經由未受安全保護的印表機，存取面向更廣的公司網路，竊取社會保險號碼、財務資訊、內部備忘錄、文件等等隱私資訊。資訊若遭竊不僅會影響公司各個員工，還可能落入競爭對手的手中，對公司的信譽造成莫大傷害。

最容易的解決方案：內建安全性功能

公司若要施展滴水不漏的安全性防護，印表機的安全性問題也不容忽略。今時今日，有些企業級印表機具備簡單易用的內建安全功能，能夠協助抵禦印表機的安全威脅。這些功能包括：

- **自動偵測威脅、保護及修復**
- **用於預防未經偵測的使用之追蹤功能**
- **PIN 或智慧卡等單一登入選項**
- **近接讀卡器機讓使用者以使別徽章方式快速驗證，並在安全的環境下使用印表機列印**
- **以安全的加密列印方式，確保敏感文件安全無虞**

下次考慮購買印表機時，無論是桌上型印表機還是多功能印表機，務必對整合性安全功能做一番調查，也別忘了啟動該些功能。藉由這樣為印表機量身打造的安全功能，就能確保公司的安全性保護措施更加嚴密，畢竟我們身處物聯網的時代，有太多存取端點要我們操心——不如主動出擊，把印表機納入防護網路之中。

在尋找更加安全的印表機嗎？
瞭解更多資訊，

來源：

[1] Spiceworks 代表 HP 針對北美、EMEA 和 APAC 地區 309 位擔任管理要職的 IT 人員進行之調查（2016 年 11 月）。

[2] <印表機安全性：您的公司資料是否真的安全無虞？>2016 年 6 月 1 日《*Computerworld*》
http://www.computerworld.com/article/3074902/security/printer-security-is-your-companys-data-really-safe.html

[3] <網際網路中，印表機是安全性最為脆弱的裝置>2016 年 9 月 8 日《*The Register*》
http://www.theregister.co.uk/2016/09/08/the_least_secure_things_on_the_internet/