疫情改變工作環境，防資安破口於未然

資料來源：法務部調查局清流月刊
作者：華梵大學資管系特聘教授 ── 朱惠中

摘要：

為提昇數位化時代的競爭力，越來越多關鍵基礎設施的運營科技（OT）正在與資訊科技（IT）融合。

OT 設備連接到 IT 網路， 同步帶來新風險

近年來，在提高運營效率的目標下，越來越多關鍵基礎設施（Critical Infrastructure, CI）的運營科技（Operational Technology, OT）被資訊科技（Information Technology, IT）系統取代。然隨著越來越多的 OT 設備連接到 IT 網路時，亦同步帶來了新的漏洞和風險，並增加網路攻擊（Attack Surface）機會，此一現象將迫使管理者尋求新安全策略和網路架構，期能提供 CI 維運者及使用者可行的策略與方法，以提昇 CI 的安全強度，特別是 OT 安全的變化和風險管理的有效性。

強化資安，從瞭解 OT 與 IT 開始

傳統上，我們將工業控制系統（Industrial Control System, ICS）的操作和程序控制，稱為 OT，亦即專注於建立和維護具有實體影響的控制過程，例如製造產品的生產線現場和廠房； 而 IT 則泛指計算機和資料網路。二者的差別在於 OT 最初是在隔離和獨立的網路中執行，其目標與要求和 IT 的目標與要求完全不同；但這些傳統的定義及網路架構的布建，已開始發生變化。 特別是近期的發展，為提昇在數位化市場（Digital Market）及數位轉型（Digital Transformation）中的競爭力前提下，這些傳統上彼此獨立的運作環境正在與資訊科技融合。越來越多的產業已開始藉由部署新的工業物聯網（Industrial Internet of Things, IIOT）設備（例如自動化生控系統、智慧城市、自動化油品輸送系統等），逐步規劃將 IT 網路、數位通訊技術與設備融合到 OT 之網路與環境中。

OT 和 IT 融合後之安全挑戰

綜整國內外各專業安全機構及大資安廠商之研究報告，將 OT 和 IT 融合

後之變化與挑戰臚列如後：

一、原本是採用專屬軟硬體架構的 OT 系統，若改用 Windows 作業系統、SQL 相容的關聯式資料庫，以及乙太網路環境，就有可能會和當前 IT 系統一樣， 共同受到病毒、蠕蟲、木馬等惡意軟體的嚴重威脅，而影響到系統運作。

二、企業若想將既有的 OT 與 IT 系統整合起來，可能使得原本 OT 系統變得脆弱，這是 OT 原設計時所未考量到的安全性漏洞。

三、 融合將挑戰現有 IT 資安產品的能耐， 因為 OT 系統與 IT 系統的本質架構並不相同，所以針對 IT 系統設計的資安產品，未必能一體適用。

四、 OT 設備的操作手冊大多可公開取得，因此有意發動網路攻擊者，容易取得相關資料。

五、OT 與 IT 操作人員在解決網路風險的考量不同。IT 人員的優先事項是保護資料，他們傾向於遵循傳統的 CIA 層級來確保安全，即機密性、完整性 和 可 用 性（confidentiality, integrity, availability, CIA)；至於 OT 部分，可 用性則被擺在第一位，然事實上，安全性應凌駕於可用性之上，故 OT 團隊更應確保流程和生產收益等因素不會因網路變化而面臨風險。

六、 OT 有網路連線的企業組織，其監控和資料擷取與工業控制系統（SCADA/ ICS）架構，近 90% 都曾遭遇過安全漏洞。據美國 Gartner 公司調查顯示， 安全問題包括病毒（77%）、 內部（73%）或外部（70%）駭客、敏感或機密資料外洩（72%)，以及缺乏設備驗證（67%）等。

七、 OT/ICS、監控和資料擷取控制系統 （SCADA)，甚或連接設備（例如閥門、量表或交換機）的網路攻擊，可能會對 CI 運作，甚至人命，造成破壞性的後果。

八、OT 人員通常缺乏安全專業知識，這不僅止於自身的內部員工，還包括委外的第三方供應商及駐點服務人員。反之，資深的安全專業人員，也有很高比例不具備曾在 OT 環境工作的經驗。

如何保護新的 IT/OT 融合環境

為降低 IT 與 OT 融合後的資安風險， Gartner 公司於 2018 年 9 月曾提出 OT 安全要求架構（如圖 1)。

COVID-19 危機加速了 IT 和 OT 的融合。即使是依賴實體過程的行業，例如金融、食品和飲料、製藥、石油和天然氣電力公用事業，也必須採取分流或異地工作， 亦即允許部分 OT 員工異地或居家工作。

多數員工可能要從自己家中的個人電腦或行動裝置，橫跨網際網路連到企業內部網路，來存取公司的 IT 應用系統或網路共享檔案，以及與同事、合作廠商進行線上協同作業等。因此，企業對於整合通訊與協作的需求大增，不只是電子郵件的收發，像是雲端視訊會議、雲端總機、行動分機、多人共享的雲端檔案、群組即時通訊等，已成為企業維持業務營運所必備之通訊基礎設施。

遠距辦公時代來臨，企業如何作好資安防護？

因疫情改變資訊環境，接下來匯整企業遭遇的威脅與因應作為如次：

一、企業實施遠距辦公或混合辦公模式所部署的網路安全，須驗證使用者身分，以建立信任（Zero Trust），確保登入者經過認證。任何類型的設備及網路連接點，都能安全地連線及執行工作；使用者在雲端或網路上工作，都能受到全面保護，免於被網路攻擊。

二、 VPN（Virtual Private Network，虛擬私人網路）是用來連接個人與企業間的私人網路。根據日媒報導，在疫情期間，全球 900 多家公司的 VPN 被駭，導致居家上班者所輸入的用戶帳號、密碼、IP 等資料均流入暗網，讓有心人士可以輕易入侵企業內部竊取機密。因此，政府機關與企業應儘速修補 VPN 漏洞。

三、 居家辦公，要讓員工在家時能連上辦公室電腦並維持相同作業方式，最簡單的作法就是使用 Windows 內建的遠端桌面，惟遠端桌面長期以來都有資安風險，不該在毫無防備下開放公開存取。

四、 由於電腦暴露在家用網路下，駭客可透過網路掃描，找到開放的網路埠，也能利用暴力破解、帳號填充等方式，強行登入。

五、 企業明定員工遠距工作之具體作法：

1. 登記並追蹤所有帶回家的 IT 資產。
2. 確保存取公司內網系統時，具有防火牆過濾和身分辨識的措施。
3. 考慮要求員工簽署從辦公室外存取資料的保密協議（Non Disclosure Agreements, NDA），讓員工認知他們負有必須履行的資安責任。
4. 訓練員工管理設備和公司資料，例如不可讓孩子或配偶使用其公務相關手機或電腦，亦可要求禁止使用公共 Wi-Fi 網路（如咖啡廳、捷運站）辦公。
5. 使用公司的 IT 資產居家辦公，需要求員工遵守公司使用隨身攜帶設備 （BYOD）的規定。另經驗顯示，在家上班的時間越長，越可能在個人行動裝置上執行公務。

六、 企業降低員工居家辦公風險之作法：

1. 制訂網路安全策略，讓員工瞭解最佳實務。
2. 企業應提供防毒軟體給員工，要求安裝於家用設備。

3. 限制遠端桌面的使用：將合法的 IP 位址列入白名單，確保遠端桌面服務僅限已授權的設備使用。
4. 使用多因素身分驗證：員工從外部連進內網系統時，須通過多因素身分驗證，降低未授權存取的風險。
5. 軟體修補為最新：制定有效的修補管理策略，在合理時間內完成關鍵弱點的修補程序。
6. 限制管理員權限：勿將管理員權限授予不需要的用戶，落實最小權限原則（Least Privilege）。
7. 防範惡意軟體：禁止用戶存取已知的惡意網站。
8. 確保具有良好的備份策略：3-2-1 原則（至少備份 3 份、使用 2 種不同媒體、其中 1 份備份要存放異地）。

七、 企業保護視訊會議環境的妥當作法：

1. 全程為會議加上密碼保護。Zoom 轟炸（Zoom-bombing）之所以會干擾會議進行，原因是外部使用者取得會議 ID，且會議沒有設定密碼保護。
2. 不要在公開平臺上分享會議資訊。雖然透過社群媒體分享會議資訊很方便，但可能導致會議中斷和遭其他惡意活動干擾。
3. 善用主持人（host）功能。主持人可以管理或刪除與會者名單，或完全鎖住會議室，後者可有效地防止會議被惡意中斷。主持人還可以停用與會者的自動螢幕分享，防止惡意破壞者分享令人反感的素材。
4. 利用等候室或大廳功能，可讓主持人控制在特定時間內有哪些人可參加會議，此功能還可讓主持人檢查誰在嘗試加入會議。
5. 通知所有使用者會議是否正被錄製，以確保在涉及隱私問題時，每個與會者都在狀況內。
6. 停用檔案傳輸功能，可改用其他方法（如電子郵件）來發送檔案，以避免駭客利用聊天室功能上傳惡意檔案。
7. 視訊會議保持更新到最新版本，能修補已知漏洞。

攻擊無孔不入，面面俱到防護

數位化時代早已來臨，越來越多的工業企和關鍵基礎設施公司的 OT 正在與 IT 緊密融合中，暴露和攻擊向量可能來自任何面向，駭客入侵無孔不入，資安防護要覆蓋整個安全控制核心，機關企業才有高枕無憂的本錢。