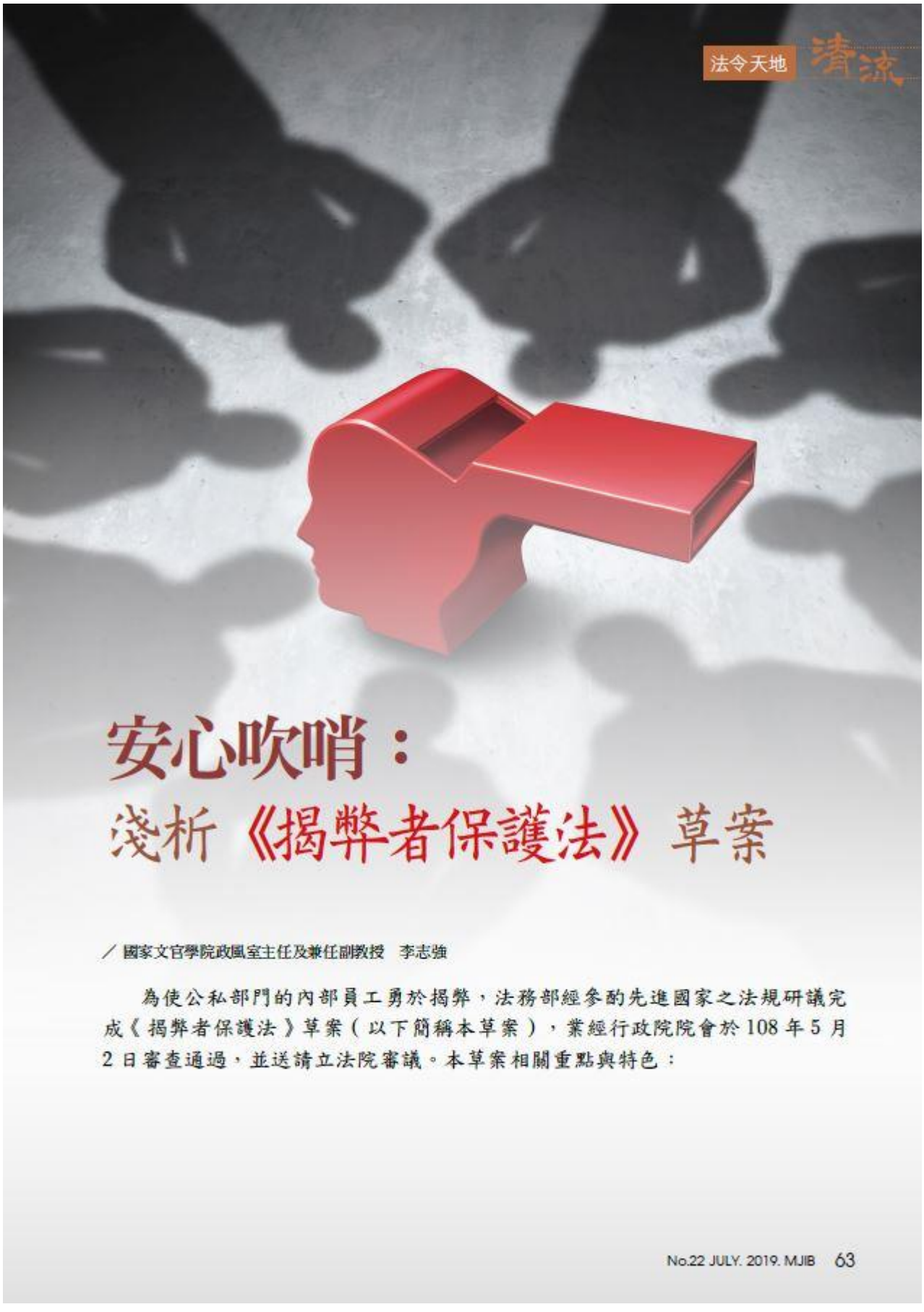
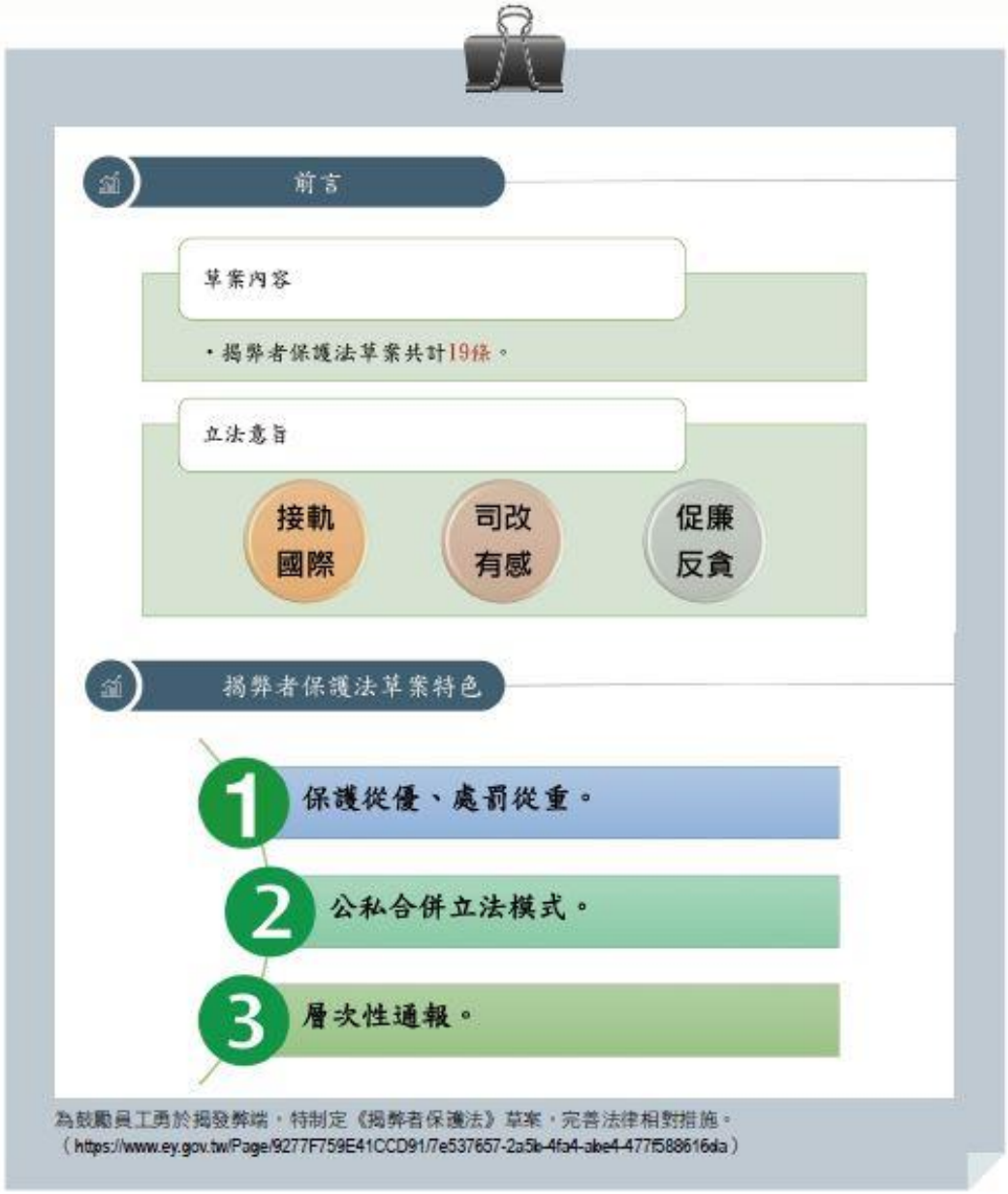
安心吹哨：淺析《揭弊者保護法》草案

國家文官學院政風室主任及兼任副教授／李志強



公私部門合併立法

為保護揭弊者，以有效打擊政府機關與私人企業內部不法行為，又鑑於弊案類型多元、案件結構錯綜複雜，公部門之弊端與私企業之不法行為界線難以一分為二，而揭弊者與被揭弊者之身分關係也非單一法律關係可以涵蓋，故為避免產生公私部門揭弊者權益之落差，本草案採公私部門合併立法之方式制定專法，而所稱之揭弊者限於機關（構）之「內部人員」，並藉此與不限內、外部人均得為「檢舉」之概念有所區別。



為鼓勵員工勇於揭發弊端，特制定《揭弊者保護法》草案，完善法律相對措施。
（https://www.ey.gov.tw/Page/9277F759E41CCD91/7e537657-2a5b-4fa4-abe4-477f588616da）

擴大揭弊保護範圍

一、在適用對象部分

揭弊之公務員採最廣義認定，即《國家賠償法》所定「依法令從事於公務之人員」，另由於承攬契約、委任契約而提供勞務給政府機關（構）之工作者，也可能得知弊案，故此等人揭弊時亦受保護，但政務官、民意代表則排除在外。在私部門之揭弊者部分，並不以具有勞務契約關係之《民法》上受僱人為限，尚包括因承攬、委任而提供勞務之人。

二、在弊端範圍部分

凡影響政府廉能之不法資訊揭露均屬之，故有關公務員貪瀆相關犯罪行為與違規行為，包括其他重大管理不當、浪費公帑、濫用權勢或對國民健康、公共安全造成具體危險之行為以及影響國計民生、危害公共健康與安全、偽造文書等。此外考量民情需求，整合社會關注公益項目，將環保、金融、食安、教育、勞動安全、社會福利、國土保育及政府採購等犯罪行為亦納為揭弊範圍。

三、在受理揭弊機關部分

包含公部門政府機關（構）之主管、首長或其指定之人、監察院、檢察機關、司法警察機關、目的事業主管機關及政風機構，私部門則為主管、負責人、董事或執行長（此即第一層受理揭弊機關），而揭弊者得依其身分別或揭弊內容之特殊限制，在數個有權受理機關中擇一提出揭弊，但若涉及《國家機密保護法》所定之機密等級事項者，僅限於向檢察機關及監察院具獨立性之機關為之。另將具外部監督功能的民意代表、媒體及民間公益團體列為第二層受理揭弊機關，以作為第一層揭弊失靈的補正措施。

禁止不利人事措施

由於公私部門弊案多為掌握內部資訊的員工始能知悉，而發生揭弊事件將恐損及特定人權益及任職機關（構）之聲譽，致揭弊者可能遭受解僱、降級、減薪等報復對待，因此本草案之重點在於維護揭弊者之權益，說明如下：

一、在保護對象部分

不限於「揭弊者」本人，尚擴及於配合調查、擔任證人，弊案發生時不願意同流合污者，及揭弊者因遭受不利人事措施提起救濟後，二度遭受不利人事措施者。

二、在不利人事措施部分

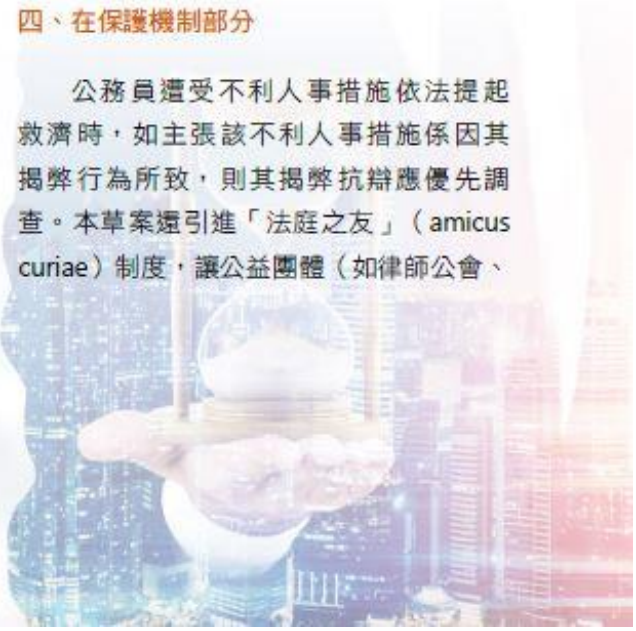
指對揭弊公務員施以懲戒、懲處或懲罰，還有對揭弊者解職或解約、降調、不利於其身分、官職等級、俸給薪資、獎金之處分、或特殊權利之調整（如專用辦公室、停車位、免簽到簽退等職場上之特別禮遇或權限），還包括受訓機會、工作條件、職務內容等之不利變更，甚至將故意揭露揭弊者身分列入不利人事措施之範疇。不僅機關（構）或雇主違反不利之人事措施者無效，還賦予揭弊者發動回復原狀或損害賠償等請求權，以及訂有禁止內部人員揭弊條款該約定無效等規定。

三、在舉證責任部分

對不利人事措施是否無效之爭議，應先由受不利人事措施之內部人員釋明，但任職機關（構）或其主管或雇主證明縱無該等行為，其於當時仍有正當理由採取相同之人事措施者，則不在此限，藉此兼顧雙方權益。

四、在保護機制部分

公務員遭受不利人事措施依法提起救濟時，如主張該不利人事措施係因其揭弊行為所致，則其揭弊抗辯應優先調查。本草案還引進「法庭之友」（amicus curiae）制度，讓公益團體（如律師公會、



公益團體、同業公會、工會或檢察署）得針對事實與法律表示意見，以協助法院妥適認定事實與適用法律。

五、在救濟程序部分

為使法律關係早日確定且避免事證消失，未具公務員身分之揭弊者發動回復原狀或損害賠償等請求，應於知悉事實發生日起6個月內，向普通法院為之，而前項之期間屆滿後，不妨礙依《民法》或其他法律所得行使之權利。若私部門恢復內部人員之職務顯有困難，勞雇雙方得以合意方式協商解決爭議，乃為避免受僱人於合意內容協議時處於弱勢，就合意內容明定最低保障之宣示規定，除3個月以上之補償金總額外，還包括資遣費、退休金。內部人員若為政府機關（構）、法人或團體編制內支領俸（薪）給而訂有委任契約者，得準用前述規定請求3個月以上之補償金，但契約約定有利於內部人員者，從其約定。

六、在違者處置部分

公務員對揭弊者施以報復性不利人事措施者，應由其任職機關（構）移送懲戒或懲處；未具有公務員身分之自然人、法人、團體者，由各目的事業主管機關處新臺幣5萬元以上5百萬元以下罰鍰，藉以發揮懲戒嚇阻效果。

《揭弊者保護法》草案制定各項工作權保護措施，避免揭弊者因揭弊行為損害工作權益。
（https://www.ey.gov.tw/Page/9277F759E41CCD91/7e537657-2a5b-4fa4-abe4-477f588616da）

有效減免法律責任

為釐清揭弊者揭弊時若向受理揭弊機關洩漏依法應保密之事項者，是否屬《刑法》第 21 條之「依法令之行為」而不罰之爭議，本草案規定，揭弊者向受理揭弊機關之陳述內容涉及國家機密、營業秘密或其他依法應保密之事項者，不負洩密之民事、刑事、行政之懲戒責任，其因揭弊向律師徵詢法律意見者，亦同。另定有寬裡反條款，即揭弊者若有出庭做證且符合《證人保護法》之情形，得享有刑責減免之適用；另揭弊者因正犯或共犯行為經判決有罪，仍不影響其得受保護之權益，同時鼓勵正犯或共犯中之公務員勇於揭弊，故保障其免職後申請再任公職之權益。

周延建立保護措施

揭弊者本人或其配偶、直系血親或其他身分上或生活上有密切關係之人，得依法施以人身安全之保護措施。若意圖妨害或報復揭弊者揭發弊端、配合調查或擔任證人，對於揭弊者及其密切關係之人實施犯罪者，則加重刑罰。另受理揭弊機關及其承辦調查或稽查人員，對於揭弊者之身分應予保密，非經揭弊者本人同意，不得無故洩漏於被揭弊對象或他人。

結語

為保護並鼓勵內部員工勇於揭發不法，英、美、日、韓等先進國家多已定有揭弊者保護法案，可見制定專法係為反貪腐及打擊不法之重要機制，同為國際間衡量國家廉能之重要指標。本草案未來立法施行後，將可解決當前保護不周或法規競合等缺憾，最重要的是強化保護機制可降低揭弊者心中恐懼，進而安心吹哨，不僅可以提高定罪率，對於不法之徒以及公私部門亦會產生監督及嚇阻效果。

本文摘自清流雙月刊中華民國108年7月 號P63-P68

疫情改變工作環境，防資安破口於未然

華梵大學資管系特聘教授／朱惠中

疫情改變工作環境，防資安破口於未然

◆ 華梵大學資管系特聘教授 — 朱惠中

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。

新的工業物聯網即是將 IT 網路、數位通訊技術與設備融合到 OT 之網路與環境中。

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；[1] 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：[2]

[1] Fortinet Taiwan 電子報，https://m.fortinet.com.tw/site/%E8%A7%A3%E6%B1%BAit%E5%92%8Cot%E8%9E%8D%E5%90%88%E7%9A%84%E6%8C%91%E6%88%B0/

[2] https://www.ithome.com.tw/news/119553

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。

OT 系統原是採用專屬的軟硬體架構，和 IT 系統整合後，將與 IT 系統一樣，同樣會受到病毒、蠕蟲、木馬等惡意軟體的嚴重威脅。

IT 人員的優先事項是保護資料，他們傾向於遵循傳統的 CIA（即機密性 confidentiality、完整性 integrity、可用性 availability，簡稱為 CIA）層級來確保資料安全。

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）。[3]

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：[4]

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；

[3] OT Security Best Practice, Gartner 2018.

[4] 安碁公司「資安認知宣導課程」講義：Securing the New IT/OT Reality Galina Antova, 2020.

圖 1　Gartner 公司提出的 OT 安全要求

Source: Gartner.

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。

企業實施遠距辦公時須驗證使用者身分，並確保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。

員工應避免使用公共 Wi-Fi 網路辦公，降低公司資訊暴露的風險。

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。

企業使用視訊會議時應保持更新到最新版本，以及持續修補已知漏洞。

安全團隊需要能夠識別和追蹤跨越 IT/OT 邊界的威脅。

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，越來越多的工業企業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。

本文摘自清流雙月刊中華民國110年11月 號P57-P63