從勒索軟體談關鍵資訊基礎設施防護

◆ 行政院環境保護署政風室科長 — 李志強

關鍵基礎設施之設備，莫不倚賴網路系統傳遞資訊，一旦網路失靈或遭到駭客入侵，將嚴重影響關鍵基礎設施之正常運作，甚至危及民眾生命財產與國家安全。

何謂關鍵基礎設施防護？

關鍵基礎設施（Critical Infrastructure, CI）領域，係依行政院國土安全辦公室於2018年修訂之《國家關鍵基礎設施安全防護指導綱要》內容所揭示（圖1）。另依《資通安全管理法》第3條第7項所提出之CI定義為：實體或虛擬資產、系統或網路，其功能一旦停止運作或效能降低，對國家安全、社會公共利益、國民生活或經濟活動有重大影響之虞，經主管機關定期檢視並公告之領域。

圖 1　我國 CI 包含 8 項主領域及 20 項次領域

而關鍵基礎設施安全防護（CI Protection, CIP），則指維護 CI 正常運作之相關政策與作為，其目標在於：

一、維護國家與社會重要功能持續運作，確保攸關國家安全、政府治理、公共安全、經濟及民眾信心之基礎設施與資產之安全。

二、以全災害[1]為安全防護考量，掌握設施相依關係，辨識潛在威脅與災害影響，降低設施脆弱性，縮減設施失效影響範圍與程度，提高應變效率並加速復原。

三、促進夥伴關係，健全跨領域、跨公私部門合作與資訊分享，進行實體、資

[1] 指天然災害、資安攻擊、意外事件、人為攻擊、非傳統攻擊及軍事威脅等災害，係 CI 辨識風險與威脅之主要依據。

通訊以及人員的保防與安全防護，預防因應各類災害所造成的衝擊影響，強化設施的安全性與耐災韌性[2]。

何謂關鍵資訊基礎設施防護？

其次，關鍵資訊基礎建設（Critical Information Infrastructure, CII），係指支持 CI 持續運作所需之重要資通訊系統或調度、控制系統，此為 CI 之重要元件（資通訊類資產）。

而關鍵資訊基礎設施安全防護（CII Protection, CIIP），即是讓 CII 正常運作之政策與作為。此部分不僅涉及領域內各機關，亦牽涉到跨領域的協同合作。申言之，由於 CI 之資訊機房及設備，莫不倚賴網路系統傳遞資訊，一旦網路失靈或遭到駭客入侵，將嚴重影響 CI 之正常運作，對於全民生命財產甚至國家安全，均可能造成重大衝擊。

資通安全已成顯學

在資訊化時代，大數據、物聯網、移動裝置及雲端服務等科技應用普及，網路與實體世界緊密結合。在高度倚賴網路之情況下，網路罪犯日益猖獗且難以杜絕，無論是竊取個人資料或商業機密，甚至駭客癱瘓公務網路系統，可謂司空見慣，若破壞 CI，後果更是難以想像，可見資通安全（Cyber Security）與民眾生活、政經穩定及國家安全等息息相關，故如何強化 CII 之安全及韌性，確屬當前重要議題。

為因應國際趨勢與新型態資安攻擊與威脅，行政院國家資通安全會報逐步提升我國資通安全防護能量，提出《國家資通安全發展方案（110 年至 113 年）》，該方案即指出網路攻擊已為資通安全顯學，經綜整全球重大網路攻擊事件，以資安事件發生之種類與多寡，分析全球相關資安事件，歸納出六大資安威脅趨勢[3]，其中即指出勒索軟體攻擊與 CII 之風險遽增。

勒索軟體攻擊實例

勒索軟體乃一種惡意程式，會加密在各種設備或系統上之文件或檔案，致使無法開啟使用，而駭客即藉機要求受駭者支付贖金，進而取得解密金鑰。勒索軟體可以進行無差別攻擊（Indiscriminate Attack），亦即駭客大規模且不加選擇地散布勒索軟體進行攻擊，或者針對性目標攻擊（Targeted Attack），如鎖定大型企業或醫療組織等行業，以脅迫取得更高之贖金。勒索軟體攻擊

[2] 指 CI 能夠降低運作中斷事故的影響程度與時間之能力。

[3] 行政院國家資通安全會報分析全球相關資安事件，共歸納出六大資安威脅趨勢，包含「個人資料與憑證外洩攻擊白熱化」、「勒索軟體攻擊風險激增」、「IoT 與行動式設備資安弱點威脅升高」、「APT 鎖定式攻擊竊取機敏資料」、「資安（訊）供應商持續遭駭破壞供應鏈安全」及「關鍵資訊基礎設施資安風險倍增」等，https://nicst.ey.gov.tw/。

資訊化時代，網路與實體世界緊密結合，由於 CI 之資訊機房及設備，莫不倚賴網路系統傳遞資訊，一旦網路失靈或遭到駭客入侵，將嚴重影響 CI 運作。

方式主要是網路釣魚，透過釣魚電子郵件或網站，誘導受害者點擊執行惡意連結與附件，或者利用資安漏洞直接傳播病毒，另亦有駭客入侵到內網後，取得管理者帳號密碼等資訊，在內網擴散勒索軟體並同時加密多臺重要主機資料。

一、美國最大燃油供應公司被勒索

2021 年 5 月間，Dark Side 勒索軟體集團攻擊美國最大燃油供應商 Colonial Pipeline 公司，致使該公司關閉所有輸送管道長達 5 天，影響美國東岸 45% 的燃料供應，美國總統拜登更因此宣布進入緊急狀態，甚至破例讓業者透過一般道路運送燃油。另根據媒體報導，Colonial Pipeline 公司在被駭的幾小時內雖然支付了數百萬美元的贖金，但卻換來了速度超慢的解密工具。

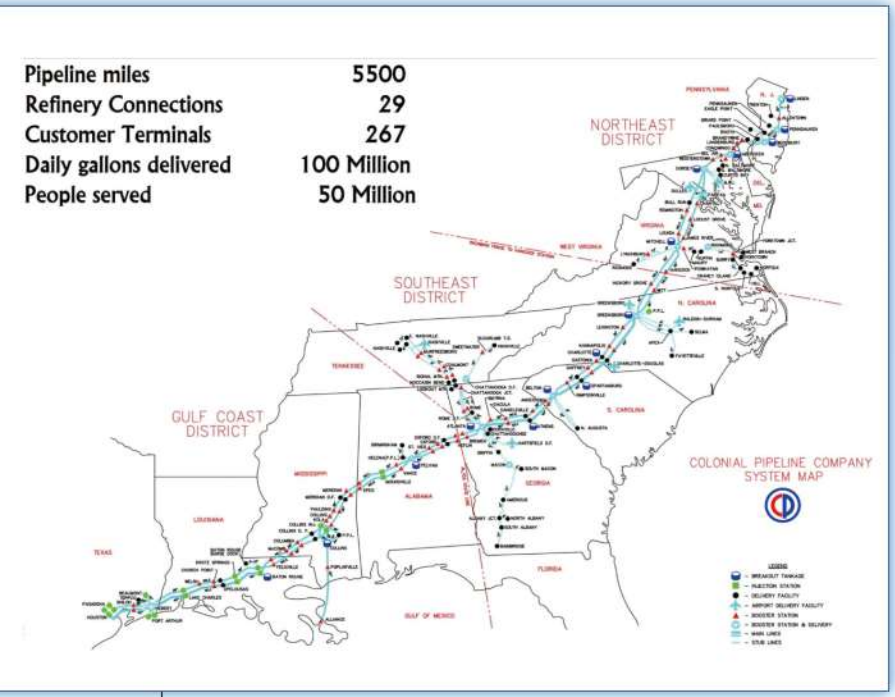
對於向駭客支付贖金之做法，官方及資安專家均不表認同，認為此舉無異於鼓勵犯罪組織未來將更肆無忌憚地向 CI 下手。對此，美國國務院在 2021 年 11 月間祭出高達 1 千萬美元獎金，鼓勵民眾舉發 Dark Side 勒索軟體集團關鍵人物之身分或位置，另外還提供 5 百萬美元獎金，給予

協助逮捕或將 Dark Side 勒索集團成員定罪之線民。

二、美國用水與污水系統被攻擊

然而，前述勒索軟體攻擊美國 CI 並非偶發事件，如美國聯邦調查局（FBI）、國家安全局（NSA）、網路安全及基礎設施安全局（Cybersecurity and Infrastructure Security Agency, CISA）與國家環境保護局（Environmental Protection Agency, EPA）在 2021 年 10 月間發表聯合公告，指出勒索軟體駭客正在針對美國用水與污水系統（Water and Wastewater Systems, WWS）處理廠展開攻擊，在 2021 年已至少發生 3 起攻擊事件，破壞 WWS 處理廠的資訊網路及各項裝置，影響提供乾淨飲用水或管理污水之能力。

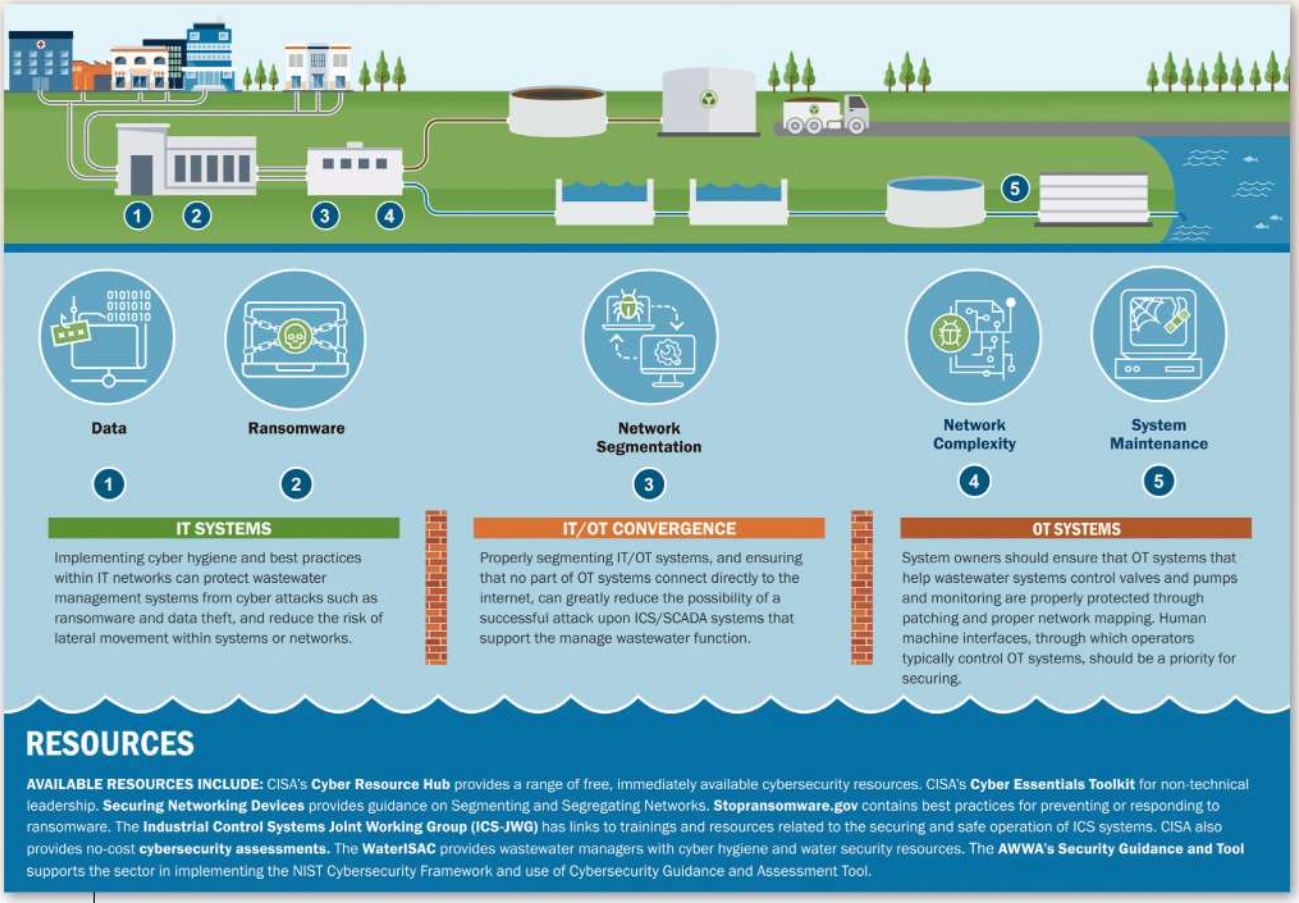
美國官方也因此針對 CI 水資源業者提供防範勒索軟體安全指引，建議 WWS 處理廠應提高警覺小心駭客入侵，如提醒員工注意網路釣魚攻擊、即時修補安全漏洞與定期更新作業系統、設置防火牆、隔離 IT 與 OT 網路，且應監控 SCDA[4] 系統之活動。



Colonial Pipeline 為美國東南部燃油的主要供應商，遭駭客攻擊後，致使該公司關閉所有輸送管道長達 5 天，影響美國東岸 45% 的燃料供應。

美國國務院在 2021 年 11 月祭出高達 1 千萬美元獎金，鼓勵民眾舉發 Dark Side 勒索軟體集團關鍵人物之身分或位置。（Photo Credit: Official FBI Twitter, https://twitter.com/FBI/status/1456344912224522241?s=20）

[4] IT 為 Information Technology（資訊技術）、OT 為 Operational Technology（營運技術）、SCDA 為 Supervisory Control and Data Acquisition（監視控制與資料擷取系統）。



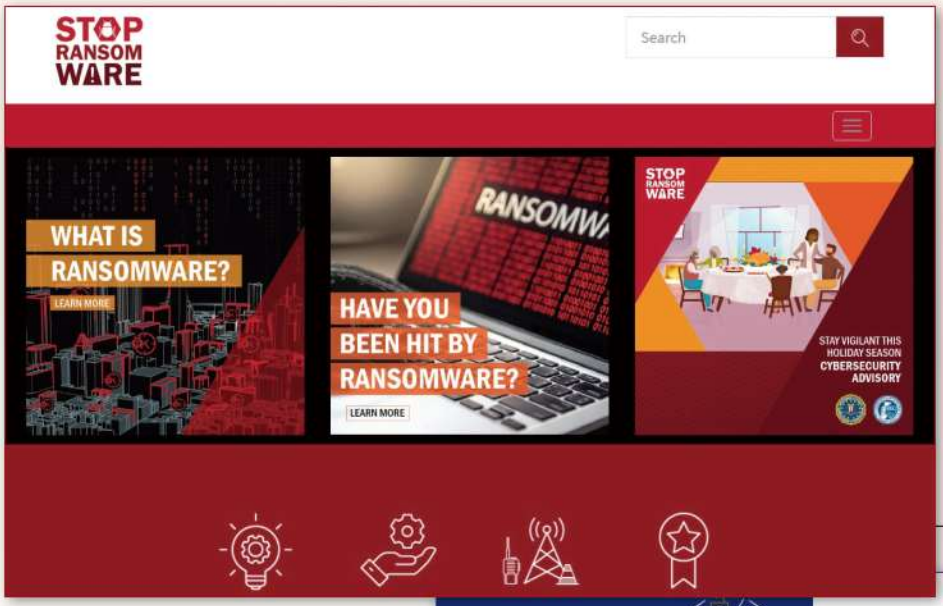
美國官方針對 CI 水資源業者提供防範勒索軟體的安全指引。（Source: CISA, https://www.cisa.gov/ncf-water）

各國之防範措施

值得注意者，為因應勒索軟體威脅，美國 CISA 整合相關情治單位設立 StopRansomware.gov 網站，除了揭露勒索軟體相關資訊外，還提供如何偵測、對抗及回應勒索軟體攻擊之指南，以增強網路防禦能力並降低勒索軟體攻擊之風險。該官方網站還提供免費健檢服務，如掃描與測試以幫助評估、識別及減少政府機關、公司企業甚至是個人所面臨之資安威脅[5]。

其實早在 2016 年 7 月，歐洲司法警察機關與資安業者就共同創立對抗勒索軟體入口網站 www.nomoreransom.org，目前已有 40 幾個國家的執法機關加入，包括我國法務部調查局、內政部警政署刑事警察局等，該網站提供超過 10 餘種勒索軟體的免費解密工具，成為全球對抗勒索軟體之重要資源網站。

[5] 其服務項目包括：1. 弱點掃描（Vulnerability Scanning）：識別容易遭受攻擊之系統或設備。2. 網路應用程式掃描（Web Application Scanning）：識別攻擊者可能利用之網站弱點與不良配置。3. 網路釣魚活動評估（Phishing Campaign Assessment）：評估員工或民眾打開惡意電子郵件（即網絡釣魚）之可能性，這係勒索軟體主要攻擊方式。4. 遠端滲透測試（Remote Penetration Testing）：通過模仿駭客之攻擊手法來測試防禦能力。5. 網絡安全評估工具（Cyber Security Evaluation Tool, CSET）：屬獨立桌面應用程式，即協助透過自我評估方式，以瞭解防禦勒索軟體事件及遭駭後之恢復能力。



美國 CISA 整合相關情治單位設立 StopRansomware.gov 網站，揭露勒索軟體相關資訊，並提供應對勒索軟體攻擊之指南。（Source: CISA, https://www.cisa.gov/stopransomware）

2016 年歐洲司法警察機關與資安業者共創對抗勒索軟體的入口網站 www.nomoreransom.org，目前已有 40 幾國的執法機關加入，該網站提供超過 10 餘種勒索軟體的免費解密工具，為全球對抗勒索軟體之重要資源網站。（Source: NO MORE RANSOM, https://www.nomoreransom.org/zht_Hant/index.html）

數位經濟浪潮來襲，提高資安意識為首要之務

當前數位經濟及資訊科技可說日新月異，世界各國皆以數位化、智慧化及網路化發展基礎建設，同時也進入情報戰、資訊戰之科技時代。隨著疫情蔓延，公私部門遠端線上作業之情況大幅增加，同時也助長了駭客攻擊。

俗話說道高一尺、魔高一丈，安裝防毒軟體固然重要，但要面對詭譎多變的駭客，提高資安意識應是首要之務，亦為防範勒索軟體攻擊之重要關鍵，尤其是良好的網路使用習慣，例如識別可疑電子郵件，不要隨意點擊連結，也不打開未知或不受信任來源電子郵件之附件。

展望未來，我國或許可以建立跨部會且整合政府資源之對抗勒索軟體入口網站，例如仿效美國官方網站 StopRansomware.gov；同時持續加強國際合作，以掌握駭客最新手法及因應之道。