Deloitte.
勤業眾信

建立關鍵基礎設施資通安全防護
亞太區工業控制系統網路安全風險調查報告

MAKING AN IMPACT THAT MATTERS since 1845

目錄

前言

關鍵基礎設施包含電力、水資源、大眾運輸以及通訊技術都是人類建造基礎社會與經濟的象徵，然而現今卻因為數位化革命導致某些關鍵基礎設施必須得跟著改變。提升工業操控技術OT以及工業控制系統(ICS)安全保護企業重要的資產維持與各產業的工業控制運作不可或缺的一環；COVID-19疫情關係更加速基礎設施資安威脅風險。

數位化革命帶動IT和OT持續融合，工業4.0高度仰賴的工業物聯網(IIoT)的運用造成工業操控技術OT以及工業控制系統(ICS)遭駭客攻擊風險正急遽上升。Deloitte亞太區資訊安全顧問團隊發現，過去10年中發生許多案例，顯見傳統的OT或ICS系統（關鍵基礎領域系統通常為十年以上系統）比以往任何時候都更容易受到攻擊。所以OT及ICS系統的基礎架構對網路攻擊的防禦能力需要進行全面而持續的強化。然而隨著IT和OT之間界限持續模糊化以及破壞式技術創新所帶來的複雜性，使得保護基礎架構環境的挑戰日益嚴峻，業者們正處於關鍵時刻。

亞太地區從社會文化、經濟發展乃至基礎建設以及科技應用充斥文化相異性，這些激烈競爭高度活躍，且地緣政治情勢充滿動盪緊張情勢的地區，反應亞洲區域在關鍵基礎建設的特殊性與多樣性。本報告檢視因快速經濟成長和科技發展下環境改變所帶來的風險，我們將重點介紹亞太區關鍵基礎設施營運業者在資安治理上，如何保護其關鍵資產免受網路威脅所面臨的挑戰，而後再深入研究如何解決相關問題，並概述有效和高效率地實現這一目標的關鍵步驟。

Deloitte亞太區資訊安全顧問團隊致力於保護關鍵基礎設施智能化時所產生資安風險挑戰，憑藉全球化資安團隊長期協助關鍵基礎設施單位處理網路資安事件和優化網路防禦能量之經驗，本報告希望提供產業管理階層(資安、營運或風險團隊)有更好的資安風險規劃與策略，提供有效的資源協助保護您的重要資產。

Sincerely,

林彥良 Max Y. Lin
亞太區工控系統資安諮詢服務負責人
Deloitte

James Nunn-Price
亞太區資安諮詢服務負責人
Deloitte

快速成長的複雜性資安風險

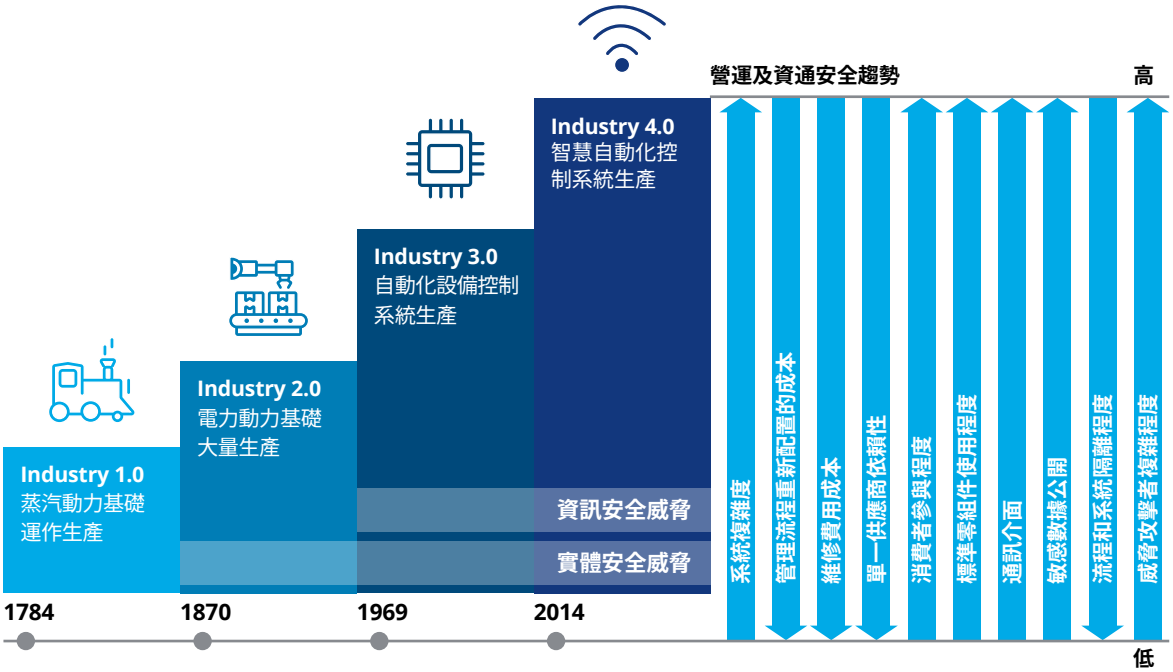
基礎設施格局日趨複雜

工業操控技術(OT)過去一直委由專責的工業控制技術團隊進行維運，多數人們認為工業控制系統（ICS）基於供應商專用協定使得其無法與其它供應商的設備進行通訊(硬體不相容以及使用不同的專用技術)，因此ICS的傳統營運基礎架構有很大程度依賴氣隙隔離（Air Gap)的先天優勢，使其不容易與傳統IT技術互通。

然而事實並非如此！真正的氣隙隔離經常運用在軍事等級等罕見的最高安全級別設施，而工廠電腦時常因未經嚴格審核即透過網際網路(Internet)進行對外連線造成很容易受到入侵並被利用來製造混亂。隨著工業系統逐漸採用通用的物聯網協定和標準，各工業系統間變得越來越相近從而使得先天優勢日漸減少，即使正確地實現了氣隙隔離，通常工廠操作上也需要工程師使用外接USB隨身碟（Stuxnet透過這種方法感染了伊朗的濃縮鈾工廠）。[1]

現今工業營運流程涉及現代化的軟體、資料和網路，需要與IT系統整合。隨著基礎建設企業（包括提供能源、水、電信、運輸和其他基礎服務的企業）進一步的數位化，使其系統和流程更加有效且可靠，IT和OT的結合幾乎可實現於各處，進而過去OT工業接控技術的緩衝區正在消失（圖1）。

圖1: 近代工業革命對資安和實體安全威脅發展



OT、ICS相關的工業控制技術

工業物連網裝置 (IIoT)

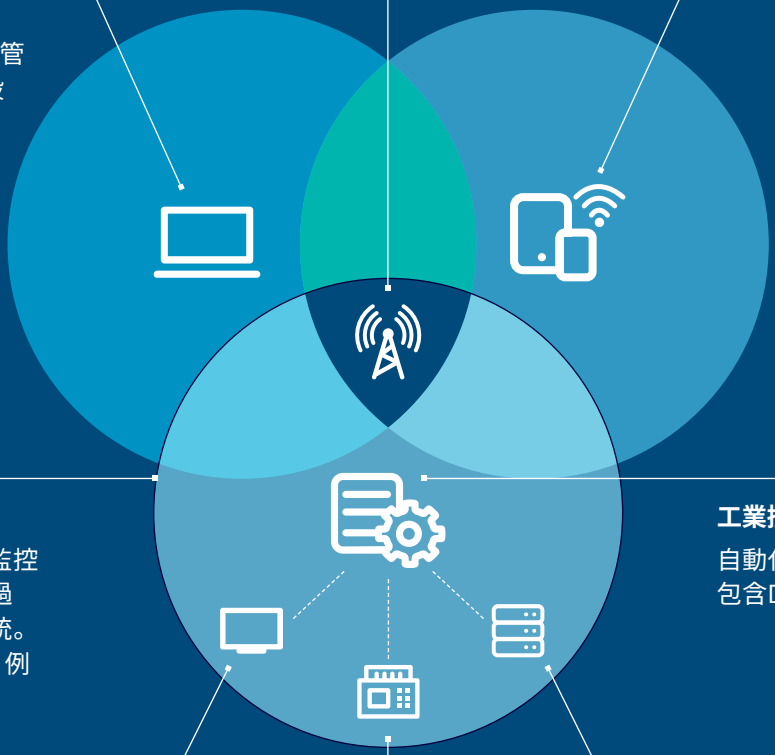
工業物連網裝置(IIoT)適用於工業環境，例如溫度監控感測器將資料傳送到雲端中分析的解決方案。 並發現有越來越多的自動化控制系統或工業環境中在使用工業4.0的概念。

資訊科技 (IT)

維持業務流程 (例如客戶關係管理和生產計畫排程) 的電腦設備、資訊設備和網路設備。

物聯網 (IoT)

通過網路進行通訊以交換資料或採取行動的連接對象和設備，例如可穿戴式設備和智慧家庭設備。



工業操控技術 (OT)

維持基礎設施、自動化系統監控和管理維運操作 (如煉油廠過程) 的系統和設備的生態系統。其中這也包括類似IT的系統，例如電腦工作站。

工業控制系統 (ICS)

自動化和控制工業過程的系統，其包含DCS、SCADA和PLC等組件。

監督控制和資料採集 (SCADA)

事件驅動的自動化控制系統體系結構特別適合於監控和控制分散於各地的自動化營運站點。

可程式邏輯控制器 (PLCs)

具備程式化運算功能的邏輯控制器，可控制與監控物理機制之工業設備(如：水泵)；PLC為自動化控制領域關鍵之組成。

分散式控制系統 (DCS)

一個控制系統中包含多個獨立子控制系統，分別在不同實際位置執行個別控制功能。唯各子控制系統間可透過通訊網路做控制資訊交換以調整如何應付系統變化。

基礎設施營運業者們正經歷工業4.0過渡期，以幫助其設施推動業務發展。工業4.0也稱為第四次工業革命，指的是工業控制系統結合先進數位科技技術進行交流分析（如：低功耗廣域網路技術(LPWAN)、4G/5G通訊、物聯網裝置、人工智慧、機器人、無人機、自動駕駛汽車、3D列印、雲端服務、量子計算或奈米科技等）並根據蒐集與分析資料進行決策，使得企業、消費者和城市變得更加靈活和迅速響應，即時做出傳統無法達到的關鍵決策。

例如性能或預測性維護分析，這些案例通常依賴於IIoT感測器將設備運作數據遠端提供給後端系統並搭配物聯網解決方案。這些技術使關鍵基礎架構營運商能夠變得更加敏捷、有效改善客戶服務，並且即時監控管理資產，一方面在於COVID-19疫情影響下，為更進一步推動這些計畫，許多營運商需要在維護工控資產和業務上盡可能遠端作業。

數位科技技術極大地增加了企業在新興科技資料和連接性要求。雖然IIoT在實現工業4.0具有巨大的潛力，但通常需要在OT資產和雲端服務之間處理大量數據，憑藉不斷擴大的相連性，帶動許多額外通訊的需求。OT和IT系統不僅整合性越來越高，而且變得越來越龐大而複雜。

綜合以上這些趨勢發展，企業面臨網路威脅更多不同層面的網路攻擊並對其OT和IT系統面臨更大的風險。隨著IT/OT邊界變得越來越複雜甚至企業也思考將內部IT服務延伸到雲端，導致針對關鍵系統進行網路攻擊的風險點正在增加。整體來說缺乏完整的治理制度，極小的弱點都能造成極大的傷害(如：系統未定期修補、網路區隔未完善實施)，即使修補程式已於多年前發布但有系統還是容易受到到常見的惡意軟體攻擊。

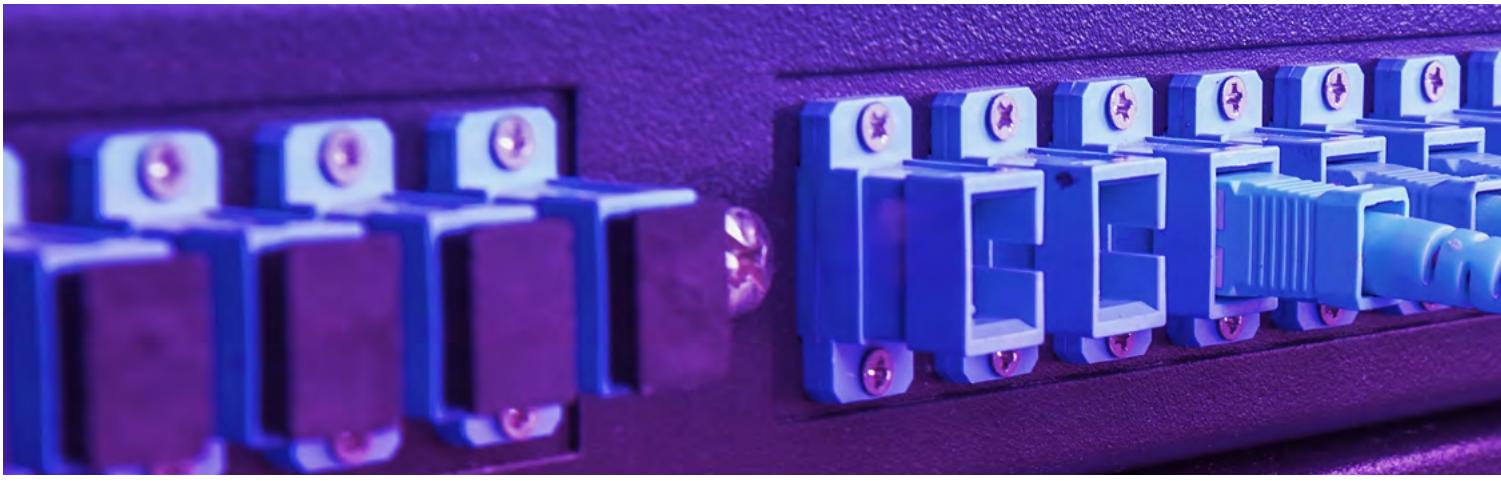
惡意軟體NotPetya攻擊案件所帶來的災難，造成了全球超過100億美元的損失，世界最大的貨櫃海運公司甚至被中斷了其全球營運，造成了高達2.5億美元的損失。如同NotPetya攻擊案所呈現的，企業正面臨了更複雜的網路安全威脅，勒索軟體甚至國家資助的網軍攻擊事件，已變得越來越普遍。

但是，網路攻擊的影響力可能不僅限於營運中斷和財務困難。回顧2015年烏克蘭電網遭到持續攻擊，所造成的整個城市電力中斷，對其基礎服務帶來的影響。這只是無數種情況之一，這些情況不僅僅限於骨牌效應，對OT系統的攻擊可能造成毀滅性後果，OT故障甚至可能直接導致人員的傷害或死亡，例如：非法關閉醫院加護病房的監護系統。2017年時，一個針對沙烏地阿拉伯一家石化廠的攻擊，造成廠內工人的人身傷害。

隨著IT / OT邊界變得越來越複雜，且網路邊界向雲端延伸，針對關鍵系統之網路攻擊的管道也正在增加

全球關鍵的基礎設施的安全性正處於危險之中，而且這種危險正在加劇。幾十年來，亞太地區一直處於相互連通的前哨，並且隨著經濟的快速增長而加速了發展。預計該地區在物聯網之部署將遙遙領先於世界，其中2024年預計將佔全球5G用戶的65%。

由於這類影響消費者和產業資訊系統的威脅事件呈指數級成長，因此有絕對必要研究如何應對現有和迫在眉睫的安全挑戰。ABI Research的一項研究統計預估，OT領域將以最快的速度成長，全球市場於7年期間的複合年增長率至2025年止將達到12%。勤業眾信除了在物聯網部署的方面處於領先之外，勤業眾信亞太地區在關鍵基礎設施上的網路安全支出亦將實現高額成長。面對這些令人鼓舞的預測同時，我們應同時重視如何應對以更高速度成長的風險。



確保基礎設施的安全

目前已經定義相關標準和框架，以幫助關鍵基礎架構營運業者改善其ICS的安全狀況，並為OT網路安全計畫奠定韌性基礎。

著名的網路安全標準

- ISO/IEC 62443：由國際自動化協會（ISA）委員會制定，並由國際電子技術委員會（IEC）通過的一系列旨在解決ICS安全風險之標準。
- NIST CSF：由美國國家標準技術研究院（NIST）制訂的網路安全框架（Cybersecurity Framework）包括風險管理實踐的五個支柱[11]，並出版SP800-82提供有關工業控制系統（ICS）安全控制的技術指南。
- NERC CIP：北美電力可靠性公司（NERC）的關鍵基礎設施保護強制性網路安全標準，重點關注於保護使用美國電網的北美企業的關鍵資產。
- ES-C2M2：美國能源部發布的電力網路安全風險管理成熟度模型和電力網路安全的實施指南。

世界各地的監理機構和關鍵基礎設施營運業者都在採用這些參考資料來幫助解決長期存在的網路風險。 從中國到紐西蘭，在亞太地區看到了越來越多使用國際認可的標準，而後者則基於NERC CIP和NIST CSF來製定其指南。另一個案例是澳洲，澳洲利用其特定領域的框架（例如ES-C2M2）來實現其電網網路韌性計畫（請參閱附錄：亞太地區的韌性工作重點）。

政府、企業甚至標準都在嘗試跟上與追趕對關鍵基礎架構持續發展的網路威脅。儘管這些威脅發展了數十年，但是基礎建設營運業者顯然尚鮮少有對OT系統進行全面檢查，且大多數系統仍然缺乏內建的安全控制功能。如此一來，也對傳統基礎架構（“棕色領域”）造成了雙重挑戰：一來是系統特別容易受到攻擊，同時，這類舊系統很難被保護，因為這需要將未考慮安全性的環境改造為具備安全控制。而穩定性要優先於便利性，對於基礎服務尤其如此，以最大限度地提高可靠性，並保護工人和大眾的安全是關鍵思維，關鍵的基礎建設營運業者已意識到這些目標正處於危險之中，因此被迫採取行動。

為了應對此挑戰，最新的專業網路安全解決方案，已可對傳統OT系統的網路通訊、功能和運行方式有足夠之了解，可以幫助企業確定其當前的ICS資產狀況以及其持續存在的威脅和弱點。此外，現在亦可透過OT安全準則、標準和藍圖，建立“設計安全”以建構更新的ICS架構。

在下一節中，我們將深入探討亞太地區關鍵基礎設施所面對的網路威脅和挑戰，企業如何有效應對這些挑戰，以及走上增強網路韌性的最佳道路。

亞太地區關鍵設施營運業者面臨的威脅與挑戰

亞太地區的關鍵基礎設施營運業者面臨著各式各樣且不斷增長的數位威脅，這既反映了不斷演變的地緣政治情勢也反映了一個充滿動盪、權力不平衡的區域競爭。這些威脅包括不具針對性但具有破壞力的勒索軟體，由國家資助或支持民族理想的駭客所進行精確的攻擊。要集中資源應對最艱難的數位安全風險，正確的情勢認知至關關鍵。這並非沒有企業結構和技術的挑戰，例如普遍缺乏對營運系統和流程的能見度，而這需要及早面對，以避免包含陷入困境。接下來我們開始探討一些常見的威脅和挑戰。

威脅者

國家支持與網軍團體

國家資助的駭客團體帶給基礎設施龐大的威脅，因為這些團體可以使用精密的手法，並透過進階情報和工具闖入並危害其他機構的營運系統，進而損害其資產的運作。[15]

此類型威脅者也有可能藉由破壞其他國家的資訊網路與供應網，以最大化破壞某些關鍵基礎服務，例如水、電、或瓦斯。各國也開始頻繁採取這樣的手法來增加他國在經濟、政治、或外交上的壓力。在這個情況下，亞太地區的電網即很有可能成為威脅者的下一個目標。

內部人員與第三方

關鍵基礎設施營運業者的內部人員，例如在職或離職員工、第三方承包商、供應鏈合作夥伴(甚至是在NotPetya攻擊案中看到的稅務軟體供應商)，都可能帶來重大風險。

這類威脅者經常利用監控系統的缺口與缺少有效的第三方風險管理流程(TPRM)來採取相對應的行動。舉例來說，有心人士可能將含有病毒的程式碼置入智慧電錶來擾亂或破壞電力網。當內部或第三方人士有機會接觸到公司機密或營運系統，不管威脅者有意還是無意，都增加了危害關鍵設施的風險。

駭客主義者

無國界的駭客組織可能通過阻斷服務攻擊 (DDoS) 入侵運行中的關鍵基礎設施的系統或破壞關鍵服務。

圖2 (下一頁) 概述了近期亞太地區對關鍵基礎設施網路攻擊的幾個事件。

挑戰

資安認知

許多關鍵的基礎架構營運業者因對其OT系統易受網路安全風險影響的資安認知有限。如果沒有對威脅的充分了解，他們很難在事件發生之前制定有效的應變策略。

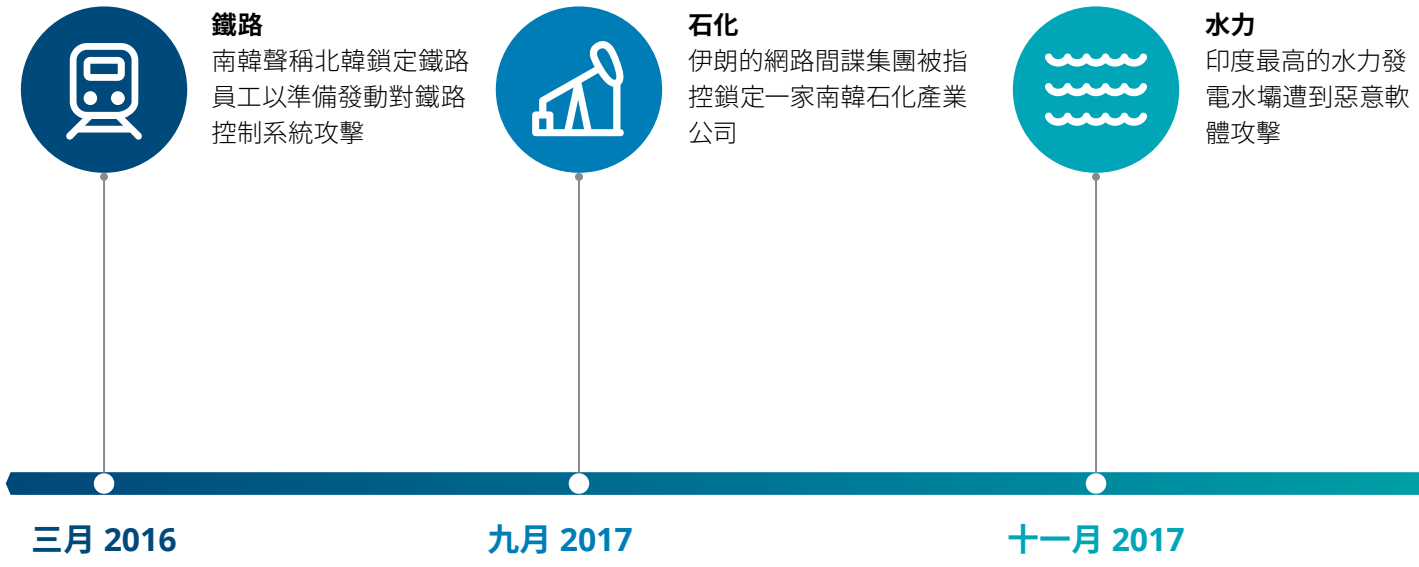
資安能見度

很少有關鍵基礎設營運業者可以充分了解其OT資產，便將其視“黑盒子”，導致對他們的OT資產如何配置或日常運行幾乎一無所知。建立精確的OT資產清單是基礎設施營運業者面臨的最大挑戰之一，但這對於評估和防範數位風險至關重要。另外，許多企業缺乏有效的監控解決方案和流程，並清楚了解其資安風險，資安能見度不足導致對OT資產無法全面了解和對情勢的認知降低，將使企業更加脆弱。

持續維護

SCADA和傳統ICS及其組件通常無法更新或缺乏適用的更新程式，即使存在，這種升級可能多年或久久才會執行。工業安全和運作可用性是營運業者的優先考量，但OT環境普遍被認會不會受網路威脅的影響，因此企業將穩定性放在比網路安全更重要的位置。但是，即使採用更激進的更新程式和維護策略，這些OT系統通常也無法適用先進的IT環境解決方案。

圖2：亞太地區基礎建設遭受的網路攻擊事件



資料來源：Deloitte analysis; news reports.[18]

挑戰 (接上頁)

網路區隔

長期以來，IT保護機敏系統的方法是將網路劃分出由防火牆或其它存取控制技術保護的安全區域。於十年前設計的工業控制環境中並非如此，當時"扁平"的網路設計並未考量網路安全性。除非設施進行重大修繕，否則不會輕易更動OT網路的基礎設施。其次由於防火牆是為IT環境而非OT環境設計的，因此它們不適用工業網路和協定(這情形已逐漸改善)。最後，資安認知不足或資安能見度不足意味著企業網路安全團隊缺乏全面的資安風險評估思維，加上沒有可靠的OT資產清單及其正確的網路架構圖，對於不熟悉的網路環境，擔心部署防火牆可能導致運作中斷的可能。

資安應變

大多數的基礎建設營運業者缺乏 (或非常有限) 針對OT系統的資安事件應變計畫，或未具備針對OT環境的操作手冊。沒有制定強而有力的流程，便無法即時對網路威脅採取全面、有效的應對措施。

資安治理

這些挑戰揭露了製定完整的OT安全治理策略的必要，以消除IT和OT團隊之間的鴻溝，與兩者間的文化差異。這並非易事，需要克服重大挑戰，包含了解OT資產和流程，並為這些資產及與其公司系統的和IT基礎設施的介面訂定網路安全角色和職責。

電力事業
網路駭客團體針對亞太地區的電力公司發動破壞力十足的Trisis / Triton攻擊。

二月 2019

核能
印度最大核能發電廠的IT網路遭到疑似北韓資助的駭客團體侵入。

九月 2019

建構關鍵基礎建設的數位防禦韌性

亞太地區的每個國家都有自己基礎建設的重點。在某些國家，金融部門、政府、甚至出口加工區也可被視為關鍵的基礎建設。在其他國家則只有能源、水和主要交通系統才被視為關鍵的基礎建設。總而言之，亞太地區政府通常將以下基礎建設分類為重要建設，不分國營事業或私人企業:

- 電力、公用事業和再生能源
- 石油、天然氣和礦產
- 水
- 電信
- 運輸，包括鐵路、航空、海運和港口。

不論各個國家的重點基礎建設為何，機構都需要整合IT / OT網路安全計畫以防範風險。為此，必須提高OT方面的安全認知，並改善營運團隊對所有OT資產的了解，從控制工作站到PLC都需要有相當程度的認知，若缺乏足夠的認識與了解，基礎建設營運業者無法獲得整體的環境可見度，進而設計一個安全的作法。在本節中，我們將探討成功的IT / OT數位安全方案。

基礎建設機構可以採用涵蓋人員、流程和技術的框架來保護其系統和資產。具備知識和工具之人員可以減輕風險、制定管理流程和應對威脅，輔以使用正確的技術檢測和分類安全弱點，機構可以有效應對挑戰，和對付前一節中所概述的威脅。

人員

有效的人員管理是建構數位安全韌性的第一步。沒有指派明確的職責，機構將很難實現其OT網路安全的目標，並且可能花費不必要的時間和資源，解決治理面的挑戰。

除了指派角色和職責，還要保持這些角色與安全目標一致。除了涉及新安全流程，也可能更改人事管理與招募的重點，或其他更其他複雜的議題。

建立抵禦網路風險的安全陣線，機構需要：

- 對企業中的每個人（從董事會到作業人員）進行OT網路風險教育訓練，以幫助他們為變革做準備
- 定義針對OT網路安全的角色和職責
- 為擔任這些職務的員工打造OT網路安全培訓流程
- 設計強大的工業網路安全和網路防禦服務，並使員工熟悉這些服務
- 建立OT網路安全工作團隊，同時在團隊成員之間建立明確規定的溝通管道。

網路安全工作團隊需要跨領域，以消除IT和OT安全之間的鴻溝。但是，如何使技能、文化和觀點不同的人員有效地合作，以應對同時涉及IT和OT的事件，或需要IT技術來支援解決OT事件的發生。IT和OT團隊之間的臨時調動有助於建立認知和建立關係，且對於定義跨領域團隊中的角色和職責十分重要。

流程

從策略到流程，如果基礎建設營運業者希望打造數位安全韌性到OT環境中，強大的流程設計，對團隊是重要的第一步。沒有明確的流程，團隊成員將很難有效地管理風險和確保營運持續。

為了設計可保護OT系統免受網路威脅的流程，企業需要：

- 定義其OT網路安全環境的當前狀態
- 訂定這些OT環境的安全目標並制定實現該目標的長期計畫，同時確保團隊成員與目標保持一致
- 識別並擬定實現目標的良好做法
- 定義可管理的評鑑標準以衡量風險降低得程度和其他成就，並明確訂定短期、中期和長期目標
- 為設計有效的OT網路安全計畫時，應取得利害關係人的認可，以幫助企業達到目標
- 使用諸如桌遊（模擬某些場景）之類的工具來開發事件應變計畫和劇本，以幫助測試流程
- 定義供應鏈管理程序並為第三方供應商制定標準以管理網路安全風險
- 開發可持續的風險管理流程，包括監控多變的數位風險、威脅和合規要求；識別及預估所需的變更；並整合所有安全功能和流程。這些可確保企業的轉型不會只是曇花一現。

所有這些流程，以及分配給企業人員的角色和職責，共同塑造OT網路治理的框架。

電力公司-Horizon Power

澳洲西岸電力公司正在發展廣泛支援智能電錶技術的即時控制分佈式能源管理系統。為了應對日益增加的網路風險，該公司運用ES-C2M2網路成熟度框架並同時導入NIST網路安全框架。Horizon Power首席資訊安全官（CISO）Jeff Campbell也非常重視將網路安全文化帶進OT團隊，包含安排OT工程師到IT安全團隊，也將他們帶到澳洲西岸政府聯合網路安全中心的會議。

技術

OT認知的網路安全技術和專門的解決方案，是幫助基礎建設營運業者保護其資產並減輕潛在風險的重要工具。對的技術可以為OT團隊操作時提供更多可見度，成為未來實施控制系統的第一步。

這些技術控制措施不應只著眼於對OT環境的邊界進行監管。為了使實現營運韌性，需要將範圍擴展到整個內部OT環境，並採取適當的控制措施來保護最關鍵的資產和系統。但是，引入新技術時也必須確保新技術不會中斷整體運作，即使是引入被動而非主動式的OT安全控制。

為了開發用於數位風險管理的技術架構，企業需要：

- 定義並詳細說明其與OT相關的網路架構、應用程式、資料庫、通訊管道和其他相關資產
- 確保具有足夠的網路安全控制和區隔
- 為內部和第三方部署安全的遠端存取技術，並針對不同角色設有特定權限
- 部署威脅偵測和追蹤方法以識別現有的威脅和持續的攻擊
- 考量在哪些特定條件下，威脅監視解決方案所檢測到的事件可能觸發ICS深度封包檢測(DPI)防火牆
- 推出權限管理工具，以有效控制對OT系統的存取
- 建立有效的安全監控系統，並透過收集和處理重要的OT來提高情境感測的能力
- 執行定期備份，並將此過程與事件應變程序整合在一起
- 建立有效的預警系統，例如誘捕系統(honeypots)，以偵測未經授權的OT系統存取

確保關鍵基礎架構免受資安威脅並非靠一人所為 而是一個專業團隊的努力達成

人員、流程和技術是建構安全基礎建設的三大支柱。保護基礎建設免受網路威脅不是一個人、一個團隊也不是一間公司能完成的工作。除了確保自身的運作，亞太地區的基礎建設營運業者將會展開彼此之間進一步的合作。由於公司、同行和政府之間的溝通有限，因此難以掌握真正的困難點並制訂正確的應對措施。但是，透過成功與失敗的案例之共享和分析，業者們可以集結努力一致對抗日益精進的。

亞太國家越來越了解這種需求。例如，新加坡最近建立了專門的OT網路安全情報分享與分析中心OT-ISAC以及特定產業的安全營運中心（SOC），以達成對基礎建設網路威脅的共識和回應。在附錄「亞太地區的數位防禦工作重點」中可了解更多資訊。

基礎設施資通安全因應策略

現在是採取行動的時候了。基礎架構營運業者需要以強大的治理框架為後盾的建立IT / OT整合網路安全計畫，以保護基礎服務和公共安全免受日益嚴重的威脅。同時，需要克服重大的傳統挑戰，為亞太地區的基礎服務的未來做好計畫。初始時這是一項艱鉅的任務，但是正確的方法將大幅減少網路風險，同時實現服務優化和業務計畫的擴展，建構關鍵基礎架構之網路安全，企業可以採取以下六個步驟：

1 定調：了解您的利害關係人	• 透過提出正確的問題，向管理階層與領導者展示直接影響營運的高風險弱點和威脅
2 定義問題：了解您獨特的立足點	• 梳理適用的法律和規範 • 找出所在位置上的影響任務成功之關鍵資產和系統等級 • 從您的營運和資產找到對應可能的網路威脅
3 了解您的立場：評估和討論您的風險	• 評估您IT和OT 網路控管的成熟度 • 找出需要優先進行網路投資的主要弱點 • 與領導階層討論評估結果
4 設定您的目標：定義您的架構	• 找出主要控制因素並闡明如何根據資產性質和關鍵程度應用 • 定義您管理目標和營運模型
5 蓄勢待發：發展您的策略	• 從快速取勝到變革性活動擬訂高收益的優先計畫 • 根據風險轉換計畫制定您的實行藍圖 • 取得董事會的支持與認同
6 試行並推廣：從小規模開始、整合、再擴大規模	• 從一個或多個代表性的網站以非侵入式控制開始試行，之後再進行調整和計畫 • 在其他關鍵資產中分階段推行

一系列針對關鍵資產和高收益計畫的實際步驟（透過關鍵績效指標之管理降低風險），將使企業關注於網路韌性和適應力的之前瞻轉型，而若能儘早讓董事會與實際營運者等利害關係人參與其中，並闡明網路適應力為確保營運安全、可靠性，及創造價值的商業的重要議題，將使整體行動順利進行。如此一來，可創造高效率、創新和新的收入來源，進而使整個企業受益。

結語

數位化革命毫無放緩的跡象，尤其是亞太地區。關鍵基礎設施以及其他與產業相關的科技，如：物聯網和預測性維護分析技術，使IT和OT的持續融合。這些科技和趨勢釋放了巨大的可能性和收益，包含提高了可靠性和效率，但同時也增加了企業對網路威脅的脆弱性。

亞太地區經濟、地緣政治風險、以及科技的多樣性反映在關鍵基礎建設中對於網路安全要求的成熟度和執行上的差異。儘管某些地區制定了法律或法規，但這些法規或規範通常側重於風險管理和監督權力。更多實現關鍵產業環境安全的特定標準和技術要求是必要的。

然而，這些對於產業的網路威脅意識正在成長。關鍵基礎設施營運業者從亞太地區甚至全球同業中意識到網路攻擊對於營運產生的嚴重影響。被攻擊不是“萬一發生”而是“何時會發生”的問題。

從政府到企業，亞太地區正在迅速加大，透過採用國際認證的網路安全標準和產業成熟度模型，加強監督和資訊共享，以確保關鍵基礎建設的安全。

許多企業剛剛開始他們的旅程，而有些企業仍在考慮前進的最佳途徑。然而，當今威脅的複雜性和力度日益增長，以及易暴露在危險中的脆弱OT系統，凸顯了陳述這些挑戰和制定針對IT和OT環境強大而實用的網路安全計畫的緊迫性。如果沒有這樣的計畫，我們的社會和經濟所仰賴的關鍵基礎建設之運作將無法得到保障。

所有關鍵基礎建設企業都不盡相同。各個產業至每個企業都會有自己獨特的網路安全要求。然而，每個企業都將從基於人員、流程和技術來制定的計畫中受益。而且，進一步的合作，只會帶給這些企業們更多的好處。當我們跨地區及跨部門的分享見解和經驗，我們將可以共同向社會的基礎服務的韌性來努力。

附註：亞太各區資通安全法規

亞太地區國家在對其關鍵基礎建設和營運上的網路威脅管理方式各不相同。有些國家長期實施了安全措施和法規來提高資安韌性，有些則還沒有健全的執行系統，而許多國家才剛開始著手找出重點營運環境中的風險。以下我們介紹了多個亞太地區國家所做的努力，包含適用於公共部門和私人企業的關鍵基礎建設的OT網路安全現行的法條、規範、和監督架構。

澳洲

澳洲政府於2017年創建了關鍵基礎設施中心，並利用《2017年電信和其他立法修正案》和《2018年關鍵基礎設施安全法》引進了適用於電信、電力、天然氣、港口和水務部門的監督架構。這個議題因而成了多數關鍵基礎設施企業首席資訊安全官、執行長和董事會的主要課題。他們及其企業可以利用許多有用的措施以深入了解其關鍵關鍵基礎建設中網路安全的意涵。

澳洲能源市場營運商最近發布了澳洲能源產業網路安全指南，該框架利用了ES-C2M2框架為基礎，以使營運商更清楚了解其當前的電力網路安全環境以及建議安全成熟度評估的工具。 儘管該框架主要針對能源公司，但亦可適用在其他關鍵基礎產業業者（例如自來水公司）的網路安全評估。

澳洲聯邦政府正在採取其他行動來提高危機意識和增強事件應變能力，他們向所有澳洲公司提供來自澳洲網路安全中心（ACSC）和澳洲律政部的可信資訊共享網路等有用資源。澳洲通訊局也頒布了一系列策略以幫助關鍵基礎設施企業緩解網路安全事件的影響。這些策略被稱為“八大策略(Essential Eight)”，並被澳洲主要的關鍵基礎建設企業所採用。

其它基礎設施產業也採用了國際通用的標準，例如ISO/IEC 62443，以幫助處理針對OT資產的網路威脅。

中國

在中國，網路安全主要由工業和信息化部（MIIT）監督，該部協同公安局（PSB）和國家互聯網信息辦公室（CAC）合作制定和執行網路安全政策和法規。 2019年發布的網絡安全等級保護2.0 (CPCS 2.0)是一項針對所有產業的OT網路安全關鍵技術標準。CPCS 2.0響應中國網路安全法，該法於2017年生效，並概述了中國所有公共和私人企業的合規性要求。

中國關鍵基礎建設營運業者廣泛遵循上述標準和其他新興法規，建立集中管理機制，並採用ISO/IEC 62443 系列標準和NIST SP 800-82準則以更好地維護營運。

印度

《2000年資訊科技法案》（2008年修訂）[27]和《2013年資訊科技準則》[28]規範了印度企業的網路安全。《資訊科技法案》指出政府可以將支持或與關鍵基礎建設的營運相關的任何電腦資源定義成受保護的系統。

電力和公營事業、電信和運輸以及戰略和公共企業等多個關鍵基礎建設企業皆根據國家重要資訊建設保護中心（2014年成立）發布的《保護國家重要資訊關鍵基礎建設指南》29開展業務。這些指南內容涵蓋了整個網路安全生命週期，包括計畫、實施、營運、災難復原和企業永續性計畫，也包含回報和負責單位。

日本

《2014年網路安全基本法》[30]是日本的主要設定網路安全、目標和政府責任的法律。《基本法》還設立了網路安全戰略總部，該總部於2015年重組了現有的國家資訊安全中心，並改成國家突發事件準備和網路安全戰略中心（NISC）[31]。NISC主責制定和協調公共及私營部門的網路安全政策，更還有一維護重要關鍵基礎建設的專案小組。

2017年4月，網路安全戰略總部發布了NISC的第四版關鍵基礎建設保護網路安全政策。[32]維護其先前政策之目的（關鍵關鍵基礎建設的保護），該政策為產業和政府提供了一個網路安全架構的準則。它著重於五個關鍵改進領域：網路安全措施、資訊共享、事件應對、風險管理和事件準備以及宣導。NISC追加了第五版的指南以建立確保關鍵基礎設施資訊安全的安全原則[33]，其中詳細說明了關鍵基礎設施營運業者和相關實體將採用的網路安全措施，以及進行風險評估的指南和工具包。

澳門

《澳門網路安全法》（MCSL）[34]於2019年12月生效。根據該法律，澳門特別行政區關鍵基礎建設的公共和私人營運業者必須履行保護資訊網路、電腦系統和控制系統的義務。 MCSL的管制範圍包括公營事業和交通運輸等使用OT、IoT和其他智能科技的部門、產業。請參閱勤業報告《澳門網路安全法（MCSL）–概述和影響分析》[35]，以進一步了解MCSL的監督要求。

紐西蘭

紐西蘭國家網路安全中心與紐西蘭控制系統安全資訊交換中心合作，制定了針對OT安全的非官方標準，主要關注電力系統和其他關鍵基礎建設企業。最新版本《控制系統作業人員自願網路安全標準》[36]於2019年發布，該標準借鑒了NERC CIP標準和NIST指南（例如：NIST CSF）。政府並於2013年發布《工業控制系統非官方網路安全標準》[37]。

這些準則是自發性、非官方的，但將來可能會成為強制性標準。於是，一些關鍵基礎建設營運業者正在依據相關指南作為自己的網路安全架構的參考[37]。

新加坡

《2018年網路安全法》[38]總體上對新加坡的網路安全進行了規範，但《重要資訊基礎設施系統的網路安全實踐準則》（CCoP）[39]專門規範了基礎設施產業的安全政策。為了遵守該準則，這些產業遵循ISO/IEC 62443、NIST SP800-37[40]、NIST SP800-30[41]、和RISK IT[42]中列出的安全架構。

新加坡網路安全局（CSA）遵循了2019年營運科技網路安全總體計畫[43]，該計畫為公共和私人企業提出了多方面的策略。該策略的重點包含：

- 開發和協調專門的OT網路安全培訓
- 建立專門的OT網路安全資訊共享和分析中心（OT-ISAC）以及不同產業專屬的安全營運中心（SOC）
- 推動公營事業與私人企業於OT網路安全創新的合作。

此外，CSA還專門針對OT環境增加強制性要求來強化上述的《重要資訊基礎設施系統的網路安全實踐準則》(CCoP)。通過這項前瞻計劃，政府能夠增強對危機和挑戰的意識，以加速基礎設施生態系統的發展，強化網路韌性、促進網路安全政策和解決方案、加強合作、推動和簡化措施，有助於企業建立OT網路安全之發展。

最新頒布的法案和強制性指南（例如CCoP）將網路安全提昇為合規要求後，此總體規劃的啟用期望能更大程度推動基礎建施企業在OT網路安全方面的努力。

南韓

《2001資訊和通訊建設保護法》[44]（2019修訂）[45]規範了韓國許多基礎設施領域的網路安全，包括國家安全、行政、公共安全、國防、金融、通訊、運輸和能源。2019年的修正案賦予中央機關更多權力可檢查那些被認為有營運重要資訊和通訊關鍵基礎建設的企業（CII企業）。根據該法案，CII企業應制定和實施入侵防禦、備份和還原等網路功能。這些動作被定義為“保護重要資訊和通訊關鍵基礎建設的措施”，由科學和資訊通訊技術部（MSIT）和政府機構每年根據CII企業的定期鑑別和其網路安全的狀況進行審查。他們還提供了弱點評估清單，以支持企業和政府機構進行檢查。

韓國的CII企業通常將“保護關鍵資通訊基礎設施的措施”、韓國網路與資訊安全管理系統以及NIST CSF，視為三個主要的網路風險管理框架。許多能源公司亦參照ISO / IEC 27002：2013[47]為根據，套用ISO /IEC 27019：2017[46]強化其工業自動化控制系統。該標準為電力、天然氣、石化相關生產、製造、傳輸、儲存和分配、生產、發電、傳輸、以及管理支援程序提供網路安全指引。

未來，關鍵基礎建設營運業者有望開始使用ISO/IEC 62443作為開發網路安全政策的參考架構，例如：化工產業將可能利用這些標準來保護OT和IIoT，同時在其生產設備中實踐智能工廠概念。電信公司在發展5G部署策略時，也同時探索其網路安全可能的選項。

台灣

台灣行政院於2014年發布了《國家關鍵基礎設施安全防護指導綱要》[48]。為了防止一般風險，台灣關鍵基礎設施公司將這一政策作為主要參考架構。儘管該指南涵蓋了一系列廣泛的風險，但網路安全仍是主要重點。2018年，行政院頒布了《關鍵資訊基礎設施資安防護建議》[49]，而該建議書主要針對OT環境提出建議

除了這些準則之外，台灣大多數公共部門和關鍵基礎建設企業適用兩項網路安全法規：《資通安全管理法》[50]和《資通安全管理法施行細則》[51]。另外六項支持網路安全管理法案之草案已對外發布，以供大眾審查和回饋。

為了遵守這些法案，台灣一些重要的關鍵基礎建設營運業者會利用行政院出版物中引用的現有準則、標準和框架，例如NIST SP 800-82、ISO/IEC 62443、NERC CIP和美國核能管理委員會制定《RG 5.71 CYBER SECURITY PROGRAMS FOR NUCLEAR FACILITIES》[52]核能設施網路安全指引提供管理框架參考。

參考資料

1. Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," *Wired*, July 11, 2011.
2. Deloitte Insights, *The Fourth Industrial Revolution: At the intersection of readiness and responsibility*, 2020.
3. Repository of Industrial Security Incidents (RISI) Database, "Steel plant infected with Conficker," accessed March 18, 2020.
4. Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2018; Deloitte, "All hands on deck: Supporting Maersk as it recovers from a global cyber attack," accessed March 25, 2020.
5. Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016.
6. Nicole Perlroth and Clifford Krauss, "A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try.," *The New York Times*, March 15, 2018.
7. GlobalData, "Asia-Pacific will lead 5G technology adoption by 2024, says GlobalData," January 13, 2020.
8. ABI Research, *Critical Infrastructure Protection (CIP) Market Size, Share & Trends Analysis Report By Security Type (OT, IT), By Services (Consulting, Risk Management, Managed), By Application, And Segment Forecasts, 2018 - 2025*, 2018.
9. Ibid.
10. International Society of Automation, "New ISA/IEC 62443 standard specifies security capabilities for control system components," accessed February 20, 2020.
11. National Institute of Standards and Technology, "Cybersecurity Framework," accessed March 24, 2020.
12. Keith Stouffer, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, Adam Hahn, "Guide to Industrial Control Systems (ICS) Security," *NIST Special Publication* 800-82 Revision 2, May 2015.
13. North American Electric Reliability Corporation, "CIP Standards," accessed March 18, 2020.
14. Office of Cybersecurity, Energy Security, And Emergency Response, "Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)," accessed March 18, 2020.
15. Dragos, "Threat Proliferation in ICS Cybersecurity: XENOTIME Now Targeting Electric Sector, in Addition to Oil and Gas," June 14, 2019.
16. Greenberg, "The Untold Story of NotPetya"; Deloitte, "All hands on deck".
17. Nick Hunn, "How to Hack a Smart Meter and Kill the Grid," October 8, 2018.
18. Reuters, "S. Korea accuses North of hacking railway systems and officials' phones," March 8, 2016; Jacqueline O'Leary & al., *Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware*, FireEye, September 20, 2017; Utpal Bhaskar, "India's power industry comes under increasing cyberattacks from hackers," *Livemint*, September 11, 2019; Dragos, "Threat Proliferation in ICS Cybersecurity: XENOTIME Now Targeting Electric Sector, in Addition to Oil and Gas," June 14, 2019; Binayak Dasgupta and Sudhi Ranjan Sen, "Cyber attack at Kudankulam; critical system safe," *Hindustan Times*, October 30, 2019.
19. Critical Infrastructure Centre, "Critical Infrastructure Centre," accessed March 18, 2020.
20. Critical Infrastructure Centre, "Telecommunications Sector Security," accessed March 18, 2020.
21. Critical Infrastructure Centre, "Security of Critical Infrastructure Act 2018," accessed March 18, 2020.
22. Australian Energy Market Operator (AEMO), "AESCSF framework and resources," accessed March 22, 2020.
23. Australian Cyber Security Centre, "Australian Cyber Security Centre," acessed March 22, 2020.
24. Trusted Information Sharing Network, "Trusted Information Sharing Network (TISN) for Critical Infrastructure Resilience," accessed March 5, 2020.
25. Australian Cyber Security Centre, *Essential Eight Explained*, April 2019.
26. Deloitte, "A new era for Cybersecurity in China," accessed March 10, 2020.
27. Ministry of Electronics & Information Technology, "Information Technology Act 2000," accessed March 18, 2020.
28. The Indian Computer Emergency Response Team, *Information Technology Rules 2013 (CERT-In Rules)*, January 16, 2014.
29. National Critical Information Infrastructure Protection Centre (NCIIPC), *Guidelines for the Protection of National Critical Information Infrastructure*, January 16, 2015.
30. Ministry of Justice, "Basic Act on Cybersecurity," November 12, 2014.
31. National center of Incident readiness and Strategy for Cybersecurity, "About NISC," accessed March 10, 2020.

32. National center of Incident readiness and Strategy for Cybersecurity, *The Cybersecurity Policy for Critical Infrastructure Protection (4th Edition)*, April 18, 2017, (Revised July 25, 2018).
33. National center of Incident readiness and Strategy for Cybersecurity, *Guideline for Establishing Safety Principles for Ensuring Information Security of Critical Infrastructure (5th Edition)*, April 4, 2018.
34. Macau Special Administrative Region, "Cyber Security Law," 2019, accessed March 10, 2020.
35. Deloitte, *Macau Cybersecurity Law – General Introduction and Impact Analysis*, December 2019.
36. National Cyber Security Centre and the Control Systems Security Information Exchange, *Voluntary Cyber Security Standards for Control Systems Operators (VCSS-CSO)*, 2019.
37. Government Communications Security Bureau, *Voluntary Cyber Security Standards for Industrial Control Systems*, v.1.0., 2014.
38. Parliament of Singapore, *Cybersecurity Act 2018*, Bill No. 2/2018.
39. Cyber Security Agency of Singapore, "Cybersecurity Code of Practice for Critical Information Infrastructure," accessed March 12, 2020.
40. National Institute of Standards and Technology, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy – 2018," *NIST Special Publication* 800-37 Revision 2, December 2018.
41. National Institute of Standards and Technology, "Guide for Conducting Risk Assessments," *NIST Special Publication* 800-30 Revision 1, September 2012.
42. Information Systems Audit and Control Association, *The Risk IT Framework*, June 30, 2010.
43. Cyber Security Agency of Singapore, *Singapore's Operational Technology Cybersecurity Masterplan 2019*, October 1, 2019.
44. Korea Law Translation Center, "Act on the Protection of Information and Communications Infrastructure," accessed March 15, 2020.
45. National Law Information Center, "Information and Communications Infrastructure Protection Act" (Korean only), accessed March 15, 2020.
46. International Organization for Standardization, "ISO/IEC 27019:2017 [ISO/IEC 27019:2017] Information technology — Security techniques — Information security controls for the energy utility industry," accessed March 24, 2020.
47. International Organization for Standardization, "ISO/IEC 27002:2013 [ISO/IEC 27002:2013] Information technology — Security techniques — Code of practice for information security controls," accessed March 24, 2020.
48. Homeland Security Police Committee, Executive Yuan, "Protection – Eliminate potential impacts and build resilience," accessed March 18, 2020.
49. National Information and Communication Security Taskforce, "Recommendations for Cybersecurity Protection of Critical Information Infrastructure," (non-official translation), 2018, accessed March 18, 2020.
50. Law and Regulations Database of The Republic of China, "Cyber Security Management Act," 2018, accessed March 24, 2020.
51. Law and Regulations Database of The Republic of China, "Enforcement Rules of Cyber Security Management Act," 2018, accessed March 24, 2020.
52. US Nuclear Regulatory Commission, *Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities*, January 2010.

致謝

關於作者

林彥良 Max Y. Lin
亞太區工控系統資安諮詢服務負責人
+886 2 2725 9988 (ext. 7779)
maxylin@deloitte.com.tw

Etienne Janot
Senior manager
+886 2 2725 9988 (ext. 7766)
etjanot@deloitte.com.tw

主要貢獻

Karen Grieve
Director
+61 2 9322 7321
kagrieve@deloitte.com.au

蕭皓天 Bill H. Hsiao
Manager
+886 2 2725 9988 (ext. 7658)
bihsiao@deloitte.com.tw

Tommy Thompson
Senior manager
+61 8 9365 7185
phthompson@deloitte.com.au

致謝

誠摯感謝以下人員對本報告的貢獻

Matthew Holt
全球工控系統資安諮詢服務負責人
+39 049 792 7998
maholt@deloitte.it

感謝Horizon Power的資安官Jeff Campbell分享他的工業控制資安經驗

聯絡我們

James Nunn-Price
亞太區資安諮詢服務負責人
+61 428 200 542
jamesnunnprice@deloitte.com.au

林彥良 Max Y. Lin
亞太區工控系統資安諮詢服務負責人
+886 2 2725 9988 (ext. 7779)
maxylin@deloitte.com.tw

澳洲

David R. Owen
Partner
+61 2 8260 4596
dowen@deloitte.com.au

中國/香港

Boris Zhang
Partner
+86 21 6141 1505
zhzhang@deloitte.com.cn

Eva Kwok
Partner
+852 2852 6304
evakwok@deloitte.com.hk

印度

Gaurav Shukla
Partner
+91 80 6188 6164
shuklagaurav@deloitte.com

日本

Haruhito Kitano
Partner
+81 803 591 6426
haruhito.kitano@tohmatsu.co.jp

韓國

Jaewoong Lee
Senior manager
+82 2 6676 2918
jaewoonlee@deloitte.com

紐西蘭

Anu Nayar
Partner
+64 4 470 3785
anayar@deloitte.co.nz

東南亞區域

Weng Yew Siah
Partner
+65 6216 3112
wysiah@deloitte.com

臺灣

林彥良 Max Y. Lin
Partner
+886 2 2725 9988 (ext. 7779)
maxylin@deloitte.com.tw