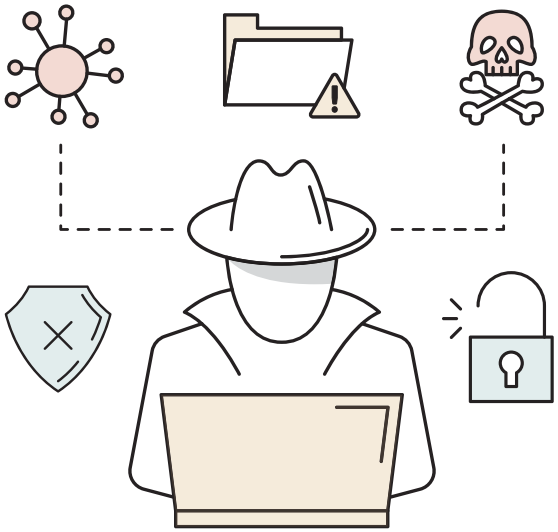
資安強化－建立縱深防禦

源起：舊系統強化

製造業的核心是工廠的維運管理，工廠的生產流程或工序主要是由工控系統 (Operation Technology，OT) 所管理控制，例如：分散式控制系統 (Distributed Control System，DCS)、資料蒐集與監控系統 (Supervisory Control And Data Acquisition，SCADA) 等，這些 OT 設備基於生產的穩定性等要求，往往作業系統或程式本身，皆經多年的未升級與更新，成爲所謂舊系統 (Legacy System) 後，其資安防護程度相對於一般的資訊系統 (Information Technology，IT)，例如：ERP、CRM、OA 等軟硬體設備，是明顯不足的，基於此本公司制定縱深防禦機制對 OT 進行強化。

病毒攻擊爲漏洞、漏洞利用、駭客威脅等三要素



第一階段

駭客（Threat）利用（Exploit）系統漏洞（Vulnerability）入侵

第二階段

潛伏了解集團架構與提升權限
制定客製化加密程序

第三階段

竊取資料後，派送加密程序，即便復原系統，也將面臨資料外洩議題。

資安政策與人員管理

1. 台聚集團自 2015 年 5 月建立 ISO 27001:2013 資安管理系統起，每年持續固定召開管理審查會議，亦敦聘外部公正單位進行集團 ISO 27001 資安制度運行審查，迄今已連續 6 年通過英國標準協會 台灣分公司 查核認證。

2. 另沿用美國國家標準與技術研究院 (National Institute of Standards and Technology，NIST) 所發展之網路安全框架 (Cybersecurity Framework，CSF)，針對該框架之識別、保護、偵測、因應與回復等五大方向，建立本公司實務上可具體執行之事前、事中與事後等 3 階段防禦體系。

   (1) 事前階段：

   進行全面性風險評估，以風險導向架構，建立資訊安全控制措施，提升安全系數。例如：訂定資安緊急應變措施與演練、社交工程演練 (一年 2 次)、OT 設備管理、每日資安回報、資安月報、資料保護與資訊生命週期管理、資安意識宣傳與資安教育訓練、法規遵循、客戶安全交易網、數位風險分析 (例如弱點掃瞄) 等。

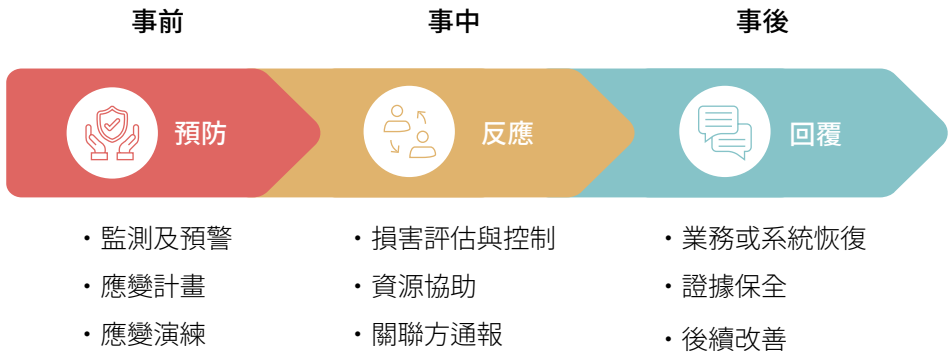
   (2) 事中階段：

   透過美國國土安全部下轄之 Computer Emergency Response Team(CERT)、台灣電腦網路危機處理暨協

調中心 (TWCERT) 及防毒廠商的通報，即時取得最新威脅情資與改善方案，深化威脅預警能力並縮短反應時間，建立預警機制。例如：資安外部威脅、日誌搜集與使用者數位足跡監控。

(3) 事後階段：

執行危機應變管理，縮短復原時間及減少衝擊，持續營運監控。例如：資安事件應變、營運持續管理、數位證據保全機制。



3. 對於近年屢造成重大損失的勒索病毒攻擊，提出整體性的持續防禦流程 (Continuous threat protection process)，以 ISO 27001 資安管理系統爲主，輔以 NIST CSF 資安管理框架，強化對風險的管控，提昇企業資安韌性並具備對資安事件承受、遏制與迅速恢復的能力，以持續提供關鍵營運服務。

4. 人員管理：定義團隊人員的角色和職責，建立抵禦網路風險的安全陣線。

(1) 對 OT 設備使用者進行 OT 網路風險教育。

(2) 撰寫 OT 資安標準書，定義安全作業流程。

(3) 建置 OT 設備管理平台，協助人員進行管理。

(4) 組建 OT 安全工作團隊，明確溝通管道。

設施與實體管理實務

1. 落實對 OT 之管理，全面針對工廠 OT 設備進行資產管理作業，包括生產商、維護商、軟硬體版本、保管人員等進行登錄，目前共納管 70 套。

2. 系統安全參數強化檢視：

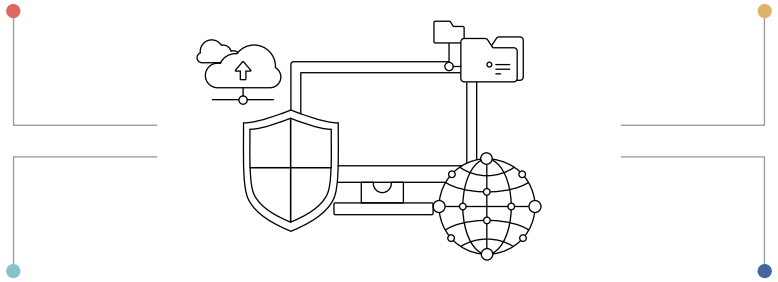
以最佳管理實務進行廠區網路設備與資安設備 (如：交換器、負載平衡設備、防火牆) 之組態強化檢核。

3. 網路縱深防禦部署：

4. 網路縱深防禦架構評估 ：

檢視配置、資訊設備安全管理規則妥適性等，評估可能風險，採取因應措施。

檢視對於持續營運所採取相關措施之妥適性。



網路縱深防禦架構評估

檢視單點故障最大衝擊與風險承擔能力。

檢視架構配置及機制有效性、網段切割與邏輯設計與各網段隔離有效性，評估可能資訊安全風險。

5. 六道防禦實務作業 ：

主動防禦：3 道

第一道防禦
強化防火牆

第二道防禦
惡意行爲偵測

第三道防禦
關鍵系統防護

被動防禦：3 道

第四道防禦
資安事件管理系統

第五道防禦
321 備份

第六道防禦
關鍵資料加密

持續管理

1. 持續從物理安全、網路安全、設備安全、作業安全、資料安全等各方面落實工控安全運行管理。

2. 逐步完善工控安全防護措施，包括上線前的安全檢測、安全能力部署、安全運行三個階段，使工控系統安全防護由原則性的部署向安全技術能力、安全管理能力的全面提升，實現管、控、防一體化。逐步從系統上線、系統運維、系統檢測等，實現工控系統安全的循環管控。