鼎新電腦

2024
製造業資安曝險
因應指南

https://www.digiwin.com/tw

2024 製造業資安曝險因應指南

數位資安守護

» 數位轉型時代如何強化營運韌性？
以新興科技助力數位創新與資安管理

» 製造業如何應對資安風暴：
更聰明、更迅速、更全面的全場域聯防

數位轉型時代如何強化營運韌性？以新興科技助力數位創新與資安管理

智慧製造、人工智慧等科技顛覆既有產業競爭規則，企業投入數位轉型的急迫感正在上升，而隨著數位轉型投入的深化，加上台灣長期深受地緣政治影響，駭客威脅與網路安全不確定性不斷升高，依據資安廠商調查台灣遭受網路攻擊的頻率，已多年為全球之最。加上疫情後，企業更加廣泛使用遠距、物聯網、新興社群行銷等工具，智慧生產、智慧工廠等企業管理營運議題發酵，也都提升了科技便利性與多重行銷管道加乘下的數位資安風險。

數位化挑戰下的資安威脅

鼎新電腦於 2023 年 3 月 ~6 月針對 2 千家上市櫃、生醫產業、供應鏈廠商與中小企業客戶，進行「資安曝險評鑑調查」，希望透過調查，讓企業客戶能夠從數位轉型視角與企業營運議題，審視目前企業資安現況。另外，2023 年生成式 AI 浪潮大舉顛覆產業既有營運規則，如同兩面刃般，在運用新興科技提取企業營運優勢與競爭力的同時，如何維持敏捷韌性適應萬變市場，重新檢視並調整資安架構與系統，厚植資安韌性，都是企業刻不容緩的課題。

鼎新電腦的資安曝險調查顯示，有 24%的上市櫃公司最擔心駭客攻擊，生醫產業、供應鏈廠商與中小企業中，有 26%最想防範勒索病毒，而企業資安規劃優先項目，上市櫃企業與供應鏈廠商對於資安軟硬體投資皆視為優先選項，其次則為人員培訓。而企業對資安需求的重點將放在組織內部共識的強化資安治理，再者是因應法規要求，以及供應鏈上下游稽核的影響。

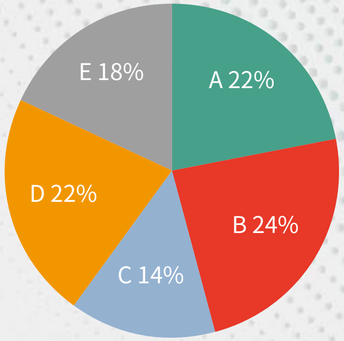
在企業資安防護已經採取的防護措施中，上市櫃企業、供應鏈廠商與中小企業僅以基礎防護 (防毒軟體、防火牆) 占比 45-49%為多，其次為郵件過濾系統 (SPAM)；而未來對於資安防禦等級可以達到何種程度？上市櫃企業希望能做到智慧防禦佔比最高，即透過 AI 持續維持資安防禦，確保防護能量最大化，生醫、供應鏈、中小企業則以可阻擋惡意程式及主流攻擊的被動防禦為最多人選擇。

企業對資安事件擔憂的項目

上市櫃最擔心「駭客攻擊」，
生醫、供應鏈、中小最想防「勒索病毒」。

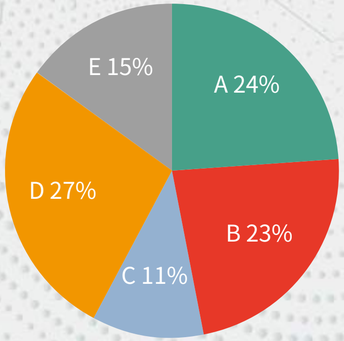
上市櫃

1.駭客攻擊
2.資料/個資外洩、勒索病毒



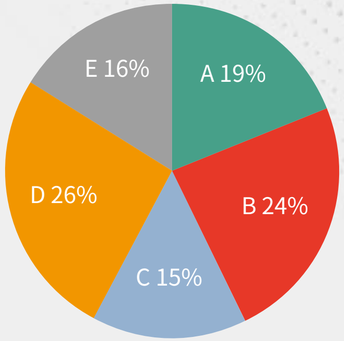
生醫

1.勒索病毒
2.資料、個資外洩



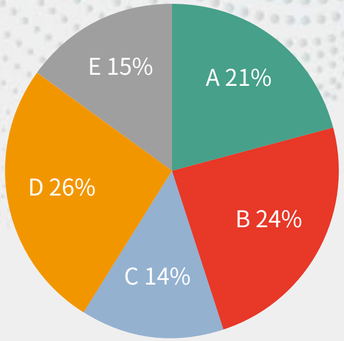
供應鏈

1.勒索病毒
2.駭客攻擊



中小

1.勒索病毒
2.駭客攻擊

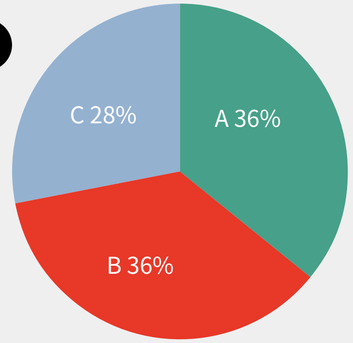


A.資料、個資外洩　B.駭客攻擊　C.人為疏失　D.勒索病毒　E.影響營運、名譽

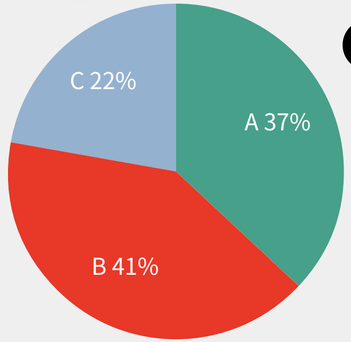
企業資安規劃優先項目

上市櫃、供應鏈，對於資安軟硬體皆視為優先規劃項目，
生醫、中小則會更重視資安軟體規劃。

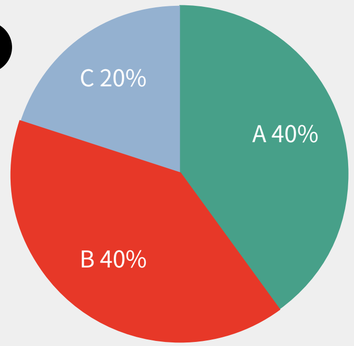
上市櫃



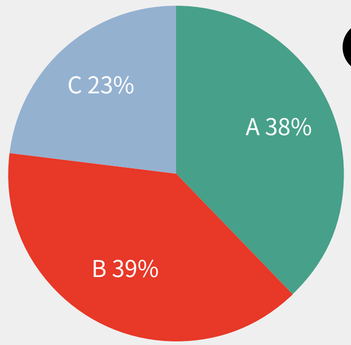
生醫



供應鏈



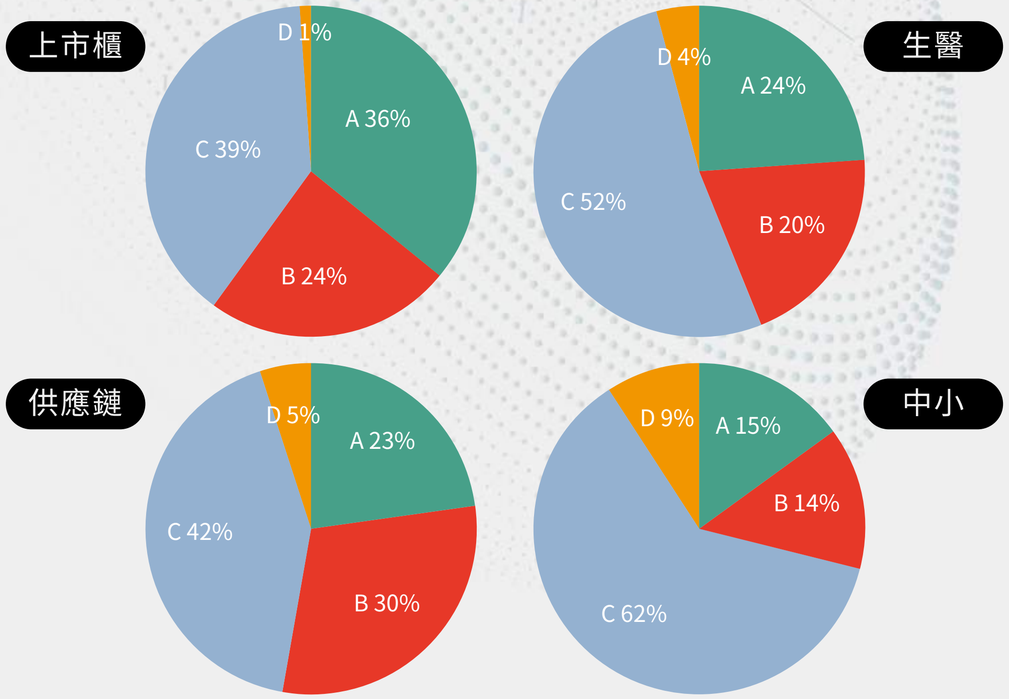
中小



A.資安硬體(如防火牆...等)　B.資安軟體(如防毒軟體、端點軟體...等)　C.人員培訓(強化意識)

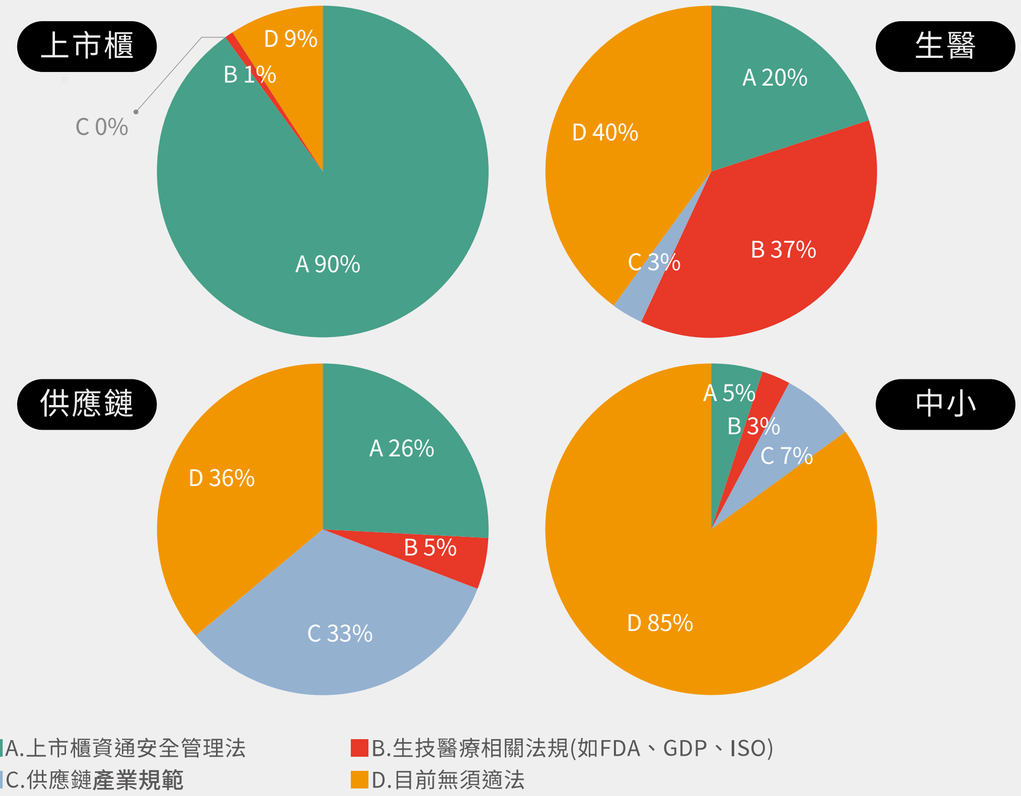
企業對資安需求來自於…

四大 TA 對資安需求皆為了強化資安治理，
上市櫃、生醫其次為因應法規要求，供應鏈上下游稽核則對其有影響。



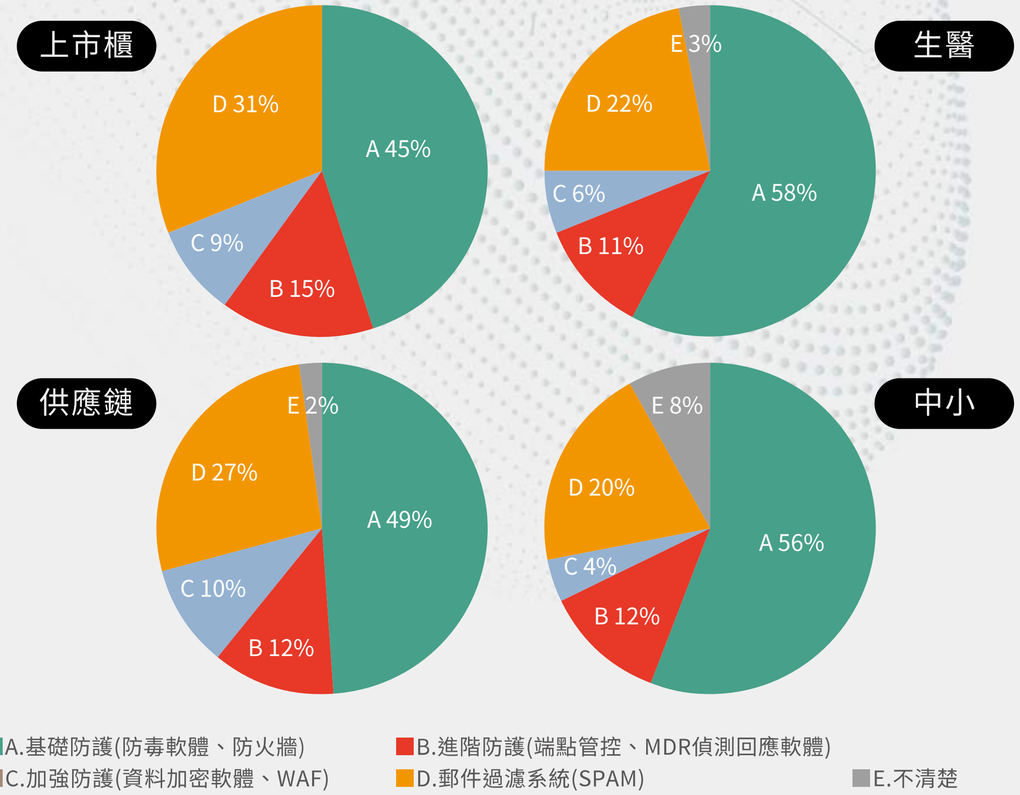
企業對於資安合規要求主要來自於…

上市櫃企業 90% 受到上市櫃資安法規要求，生醫業者約 37% 受
生醫法規要求，而供應鏈企業約有 33% 需符合各供應鏈規範要求。



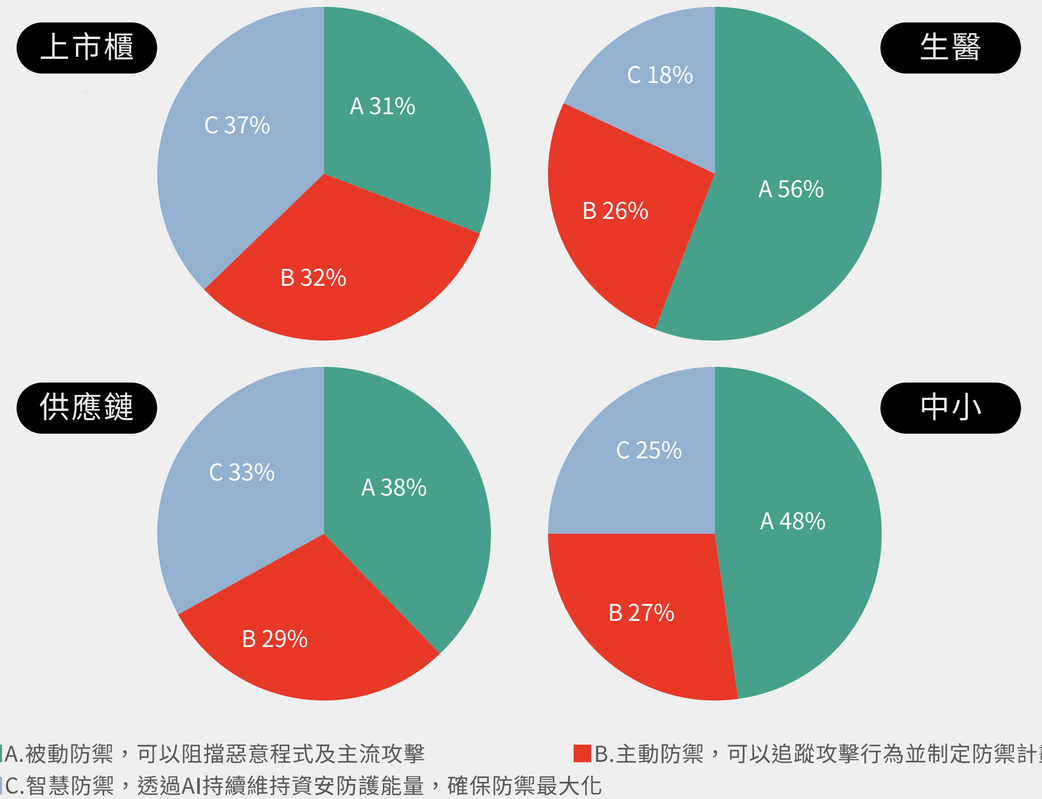
企業資安防護已採用內容

四大 TA 大部分企業有基礎防護佔比最多，
其次為郵件過濾系統。



企業對於資安防禦等級希望可以達到什麼程度

上市櫃希望能做到智慧防禦佔比最高，
生醫、供應鏈、中小則以「被動防禦」最多選擇。



機會與風險兼具：生成式 AI 將成未來 1~2 年最大的資安挑戰

《iThome》「2023 資安大調查」系列就指出[1]，社交工程攻擊在 2021 年和 2022 年為第四大資安威脅，但在 2023 年突然竄升為發生風險最高的威脅，一方面也與生成式 AI 技術的出現有關，此觀點同樣於 PWC 的《2024 全球數位信任洞察報告》[2] 得到驗證，報告發現，全球企業對於生成式人工智慧可能產生的風險準備不足。另外，因資料外洩，蒙受財務損失超過百萬美元的企業，在過去一年比例有增加的趨勢。

1 資料來源：iThome 2023 資安大調查系列 https://www.ithome.com.tw/article/156858

2 資料來源：PWC 2024 全球數位信任洞察報告 https://www.pwc.tw/zh/publications/global-insights/global-digital-trust-insights-2024.html

《遠見雜誌》的「2023 資安長大調查」[3]，全面盤點上市櫃企業的資安治理規劃，結果顯示逾半數企業資安治理程度，尚在初步發展階段，另外企業面臨資安議題最棘手之處在於人才，資安人才缺口很大，建議企業可透過與值得信賴且具規模的第三方專業資安服務廠商合作，快速強化公司的資安韌性。

委外託管維運有效降低企業資訊成本

除了資安防護，數位化轉型過程也帶來多元化的軟體應用，複雜化的硬體架構，以及數位化的數據管理，需要擁有好的機房環境、硬體設施，甚或一個資訊維護團隊，這都對企業帶來極高的成本。面對數位轉型所衍生的多樣化設備及複雜的管理方式，如何減少傳統維運相關的大量資本支出、並且節省冗餘技術的成本，讓成本符合效益，就得從合理的資訊管理思考與重視資訊管理情資著手，這是邁向數位轉型的企業於資訊管理領域的必經之路，也已經有不少企業，藉由委外託管方式、結合 AI 平台管理，優化企業的資訊系統建置與設備維護，不斷提升資安危機意識與降低可能的衝擊危害，促進企業營運發展敏捷，充分發揮數位管理及運用。

3 資料來源：《遠見》2023 資安長大調查：https://event.gvm.com.tw/2023CISO

數位化時代來臨，在產業競爭中更需要強化資安領域，提升危機意識與保護核心資訊，是無論上市櫃或中小企業都必須展現在資訊管理的決心。鼎新電腦認為，隨著大數據、AI、雲服務的崛起運用，IT 智能運維及資訊安全將會是企業未來更加重視的一環。面對無所不在的資安攻擊威脅，應從企業管理思維開始，首要先找到資安漏洞並全盤檢視企業自身需求，再來規劃資安預算、增設專職人員、找尋合適的設備和資安防禦軟體，進一步

符合法令規範，依照企業資安管理進程的不同，例如朝完善資料備份、提升資安防禦、進階到 AI 智能維運等，而有不同的資源配置，維持企業營運、重構資安策略等降低被駭客攻擊的機率和損失。

在數位轉型的進程下，企業維持競爭力的關鍵在於，如何審視可能存在的威脅與入侵路徑，尋找合適的防護工具等軟硬體升級或與資安服務廠商合作，發揮資安與運維預算綜效，甚至運用生成式 AI 的科技，同時注入資安能量，兼顧創新與安全，讓企業靈活營運，又可利用科技力量引爆營運目標，大力提升數位轉型競逐中的競爭力。

製造業如何應對資安風暴：更聰明、更迅速、更全面的全場域聯防

Fortinet《2023 上半年全球資安威脅報告》報告中顯示，光是亞太地區，在 2023 年上半年就偵測到 4,120 億次的資安攻擊，其中台灣遭受攻擊高達 2,248 億次，以佔比五成之姿成為亞太攻擊熱區，鼎新電腦資安團隊進一步分析，發現竟有 70% 的攻擊目標劍指製造業客戶。

關鍵摘要

而鼎新也在實際服務過程中，不論公司規模大小，統計了近2,000家企業，在過去一年裡皆持續遭遇惡意威脅。

經由鑑識資安事件，鼎新資安服務團隊掌握到製造業客戶既有資安環境，並不具備防禦新型攻擊的能力，關鍵問題在於：

1. 缺乏資安管理機制
2. 員工資安意識不足
3. 僅有防火牆、防毒軟體

那麼，資安該如何完善呢？

建議企業應可參照行政院國家資通安全會報技術服務中心之「資安威脅趨勢及防護策略」，鼎新也就自身服務經驗，提供下列面向以佈建資安防禦能力：

事前預防

企業應假設此時此刻正遭受攻擊，以便及時掌握已衍生的風險與攻擊旅程，並保有隨時應變的資安韌性。事前預防措施包含風險評估、弱點掃描、滲透測試、社交工程演練、資安教育訓練等。

事中偵測

企業應導入可迅速識別和阻止異常行為的入侵偵測技術與防禦系統，甚至借助人工智慧（AI）及機器學習（ML）的力量，以辨識新興的資安威脅，加強應對潛在攻擊的能力。

事後應變

當企業第一道防線的預防及主動偵測的措施都確實執行了，也需訂立完備的災害應變程序、系統備援機制等應變流程，以利提高企業針對應急情況的反應速度和效率，減少營運中斷的損失。

持續精進

已然成形的資安策略及措施是否符合現今需求且有效防禦威脅，皆需要藉由資產盤點、定期稽核與風險評估，確認資產等級、風險衝擊值對企業的影響，透過不斷學習和改進，企業可以保持高度的資安韌性，未來發生資安事件時能夠快速而有效地應對威脅。

避無可避的資安風暴

根據趨勢科技（Trend Micro）2021 年的製造業者調查，近 75% 的製造現場資安事件，曾直接或間接地導致生產線停擺，而旗下聚焦 OT 資安領域的睿控網安（TXOne Networks）也統計，若製造業遭遇勒索軟體攻擊，其自動化產線的平均停擺時間為 21 天，每次停擺的財物損失更可能高達 280 萬美元（將近新台幣 9000 萬元）。直至 2022 年，製造業受到駭客攻擊的比例達 58%，已取代金融服務業成為多數有心人士鎖定的目標。

以 2022 年的 TOYOTA 資安事件為例，其供應鏈在短時間內被駭客攻擊不下兩次，其中一次為零件供應商遭到入侵，造成 TOYOTA 的零件管理系統故障，直接影響 14 間工廠、28 條生產線，遭受牽連的產量超過一萬台車輛，無形損失則難以估計。

由 CIO Taiwan 發布的《2022 年美國版 CIO 大調查報告》中，有超過半數的受訪者指出，資安管理是資訊長最為關注的任務之一，三分之一的受訪者也直言，降低營運風險、提升企業資安仍是未來的第一優先處理事項。有 56% 的美國製造業者已提高網路安全計畫的優先程度，而 50% 以上的業者準備以資安風險管理主導 IT 專案，資訊安全的強化需求也為左右預算增減的首要原因。

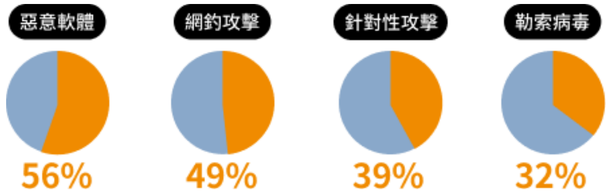
回到面向台灣的《2023 年 CIO 大調查報告》，已有六成的受訪組織派任了資安專責人員，但通常企業內主責資安的最高長官即為 CIO，因此 CIO 花費最多時間、心力的工作仍是提升資安韌性，需密切關注威脅事件與資安合規度等資安議題。傳統製造業與高科技製造業在此調查中合計佔比高達六成，顯現製造業已經更加重視資安，並超過 40% 的製造業將網路安全與資安列為重點投資項目，然而，從整體調查來看，卻有 43.3% 的企業未施行資料治理，還有 50% 以上的 CIO 困擾於員工的資安意識薄弱，如何納管 OT 資安也讓 49.4% 的 CIO 感到憂心。

單純從 CIO Taiwan 的 CIO 大調查結果而言，已有許多台灣企業準備增加資安投資，不過相較於美國企業於 2022 年便擁有布局資安的成熟意識，台灣的資安仍有進步空間。

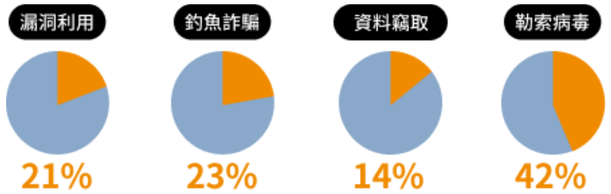
目前全台有八成以上的製造業者為鼎新合作夥伴，鼎新以企業運營的角度觀察並紀錄了相關發現，希望可以協助製造業客戶有效提升資安防護力。

製造業資安 VS 黑色產業鏈

身處科技蓬勃發展的資訊化時代，各大企業紛紛擁抱數位轉型，常被台灣民眾稱為傳產的傳統製造業，也對智慧製造、工業 4.0 等嶄新科技趨之若鶩，期望導入自動化系統工具、聯網設備後，可為企業降本提效、增加收益，然而黑色產業鏈卻同時恣意成長、茁壯，駭客能簡簡單單透過網路順藤而上，介接了新工具、還在為公司賣力運作的元老級機台，或成零時差攻擊的破口。



Fortinet 在《2023 年 OT 與網路資安現況調查報告》中，統計每家公司遭到惡意威脅的比率，顯示企業可能遇到零次或無限次的資安攻擊，比如說短時間內不限於次數或攻擊類型，也許將會同時遭遇網釣攻擊或勒索病毒，故提醒製造業者應留意上述來勢洶洶的資安威脅。時至 2023 年終，鼎新也在實際服務過程中，蒐集並觀察製造業客戶面臨資安攻擊的數據，統計了近 2,000 家企業，不論規模大小，在過去一年裡持續遭遇惡意威脅：



為什麼製造業成為駭客組織眼中的肥羊？這個問題或許可以由致力工業自動化與數位轉型的洛克威爾自動化（Rockwell Automation）來解答，《工業營運的 100+ 網路資安事件剖析》中針對直接影響 OT 與工控系統運作的資安事件進行分析：

- 多數 OT 與 IT 的界線不清，80% 的資安事件是駭客從 IT 系統入侵所致。
- 資安事件中有 60% 為營運中斷事件、40% 為存取與機敏資料外洩事件。
- 營運中斷對 供應鏈的影響 達 65% 以上。
- 公司員工資安認知較低，超過 30% 的資安事件源頭來自於內部人員 。
- 近 60% 的攻擊來自駭客國家隊所引發。

洛克威爾自動化的分析報告著墨於製造業最在乎的「可用性」，也就是營運中斷，而鼎新還要進一步提醒製造業客戶，科技大躍進助長了駭客組織及惡意程式的發展，這些懷抱他心的有心人士已不滿足於單純的惡作劇，除了引發營運中斷事件使企業因產線停擺而損失外，攻擊目的轉為更具價值的勒索贖金，補充組織銀彈以策畫更加兇惡的資安攻擊，所以擁有大量製程產權資料，以及依賴核心系統、機台設備運作的製造業就成了最佳目標，駭客還可從供應鏈途徑順藤摸瓜，藉此造就影響範圍更廣、更大的供應鏈攻擊。

鼎新在鑑識資安事件的過程中，也發現製造業客戶往往將風險暴露在虎視眈眈的駭客眼前，關鍵在於缺乏完整且強而有力的資安布局，既有的資安環境並不具備防禦新型攻擊的能力：

- **缺乏資安管理機制：**未與時俱進
- **僅有防火牆、防毒軟體：**卻自我評估已完成資安建置
- **員工資安意識不足：**使用習慣成為最大資安破口
- **系統漏洞不斷被揭露：**無法即時跟上修補
- **系統停機更新費時：**損及運營能量
- **最新導入的系統、設備：**未做足資安部署
- **機台限制第三方軟體：**難以提升資安防護

用受害者心態強化資安韌性

不限於半導體大廠台積電等高科技製造業，台灣許多製造業在全球供應鏈中都扮演著關鍵角色，並且發展至今的重要程度不減反增，因此萬萬不可輕忽越發猖獗的供應鏈攻擊。為了抵禦黑色產業鏈所帶來的資安衝擊，需要更加聚精會神地抗衡花招百出的惡意威脅，企業無不極力建置資通安全機制，以避免給予駭客與惡意程式入侵得利的機會。

過往，傳統產業在資安領域的舊思維，可能僅限於防火牆、防毒軟體，但到了現今遠遠不夠，企業應抱持著可能是受害者的心態，來面對未知的駭客攻擊，畢竟多數駭客為手法高超的頂尖攻手，有一堆法子可以「翻牆」、騙過防毒軟體，並且極有耐心地潛伏等待給企業致命一擊的機會。因此不少製造業客戶積極導入資安服務，想要降低營運風險，朝向營運不中斷的目標持續前進。

最常設置的資安方案包含了事前評估預防、備份以防範未然，事中偵測與備援確保營運不中斷，以及事後應變排除內憂外患，可以說是透過「被駭了怎麼辦」的預設立場進行沙盤推演，推敲出企業資安的致命弱點，並設計資安事件發生後的應變程序，將第一道、第二道、第三道等無數道防線，都強化得更具資安韌性。

就今年而言，便有不少鼎新服務的製造業客戶遭遇資安事件，其中最為嚴重的是日常營運所用的 DB、AP 遭加密，受害公司不僅防火牆韌體過舊、對外開放 IP 無限制連線高風險連接埠，也無安裝相關端點防護措施，導致公司業務停擺，災情慘重。而反觀導入 MDR 的製造業客戶，則能有效阻擋惡意軟體與威脅入侵，即使駭客的觸手已經伸進企業門縫之中，也能避免危害並留下入侵紀錄，以利後續評估，改善資安現況。

掌握更聰明、更迅速、更全面的資安

做為全球供應鏈的關鍵角色，台灣的製造業者不可也無法不重視企業資安，需時刻掌握敵人動向，藉由完善資安措施、蒐集威脅情資以部署資安大局。鼎新也就自身服務經驗，並參照行政院國家資通安全會報技術服務中心提供之「資安威脅趨勢及防護策略」，建議製造業客戶以下列面向佈建資安防禦能力，完善資安布局：

事前預防

企業應假設此時此刻正遭受攻擊，以便及時掌握已衍生的風險與攻擊旅程，利於建立守衛企業的第一道防線，並保有隨時應變的資安韌性。為了減少潛在攻擊面，事前預防措施應包含：

・風險評估
區分資產等級與風險衝擊值，檢視資安策略不足之處。

・弱點掃描
檢測安全漏洞和弱點，防止被有心人士利用。

・滲透測試
模擬駭客行為找尋安全漏洞和弱點，確保防禦能力。

・社交工程演練
模擬釣魚郵件、冒充身份等攻擊情境，加強員工資安認知。

・資安教育訓練
補強員工資安意識，以免使用系統的壞習慣造成後患。

事中偵測

完善了事前預防措施後也萬萬不可懈怠，如果全然信任企業資安的堅固性，恐將無法掌握絕對的安全。企業應導入可迅速識別和阻止異常行為的入侵偵測技術與防禦系統，甚至借助人工智慧（AI）及機器學習（ML）的力量，以辨識新興的資安威脅，加強應對潛在攻擊的能力。

・郵件過濾

自動過濾垃圾郵件，防禦外部威脅。

・DLP －資料外洩防護

監視、識別和保護機敏資料，防止資料外洩。

・MDR －威脅偵測與應變服務

監控與分析端點設備的異常活動，主動隔離安全威脅。

・WAF － Web 應用程式防火牆

監測、過濾網站進出流量，保有網站的安全性和可靠性。

事後應變

意外之所以稱呼為意外，就是在萬事俱備的情況下也可能發生料想不到的事，因此當第一道防線的預防及主動偵測的措施都確實執行了，也需訂立完備的災害應變程序、系統備援機制等應變流程，以利提高企業針對應急情況的反應速度和效率，減少營運中斷的損失。

・備份機制

恢復在復原點目標（RPO）保存的備份，使公司維持日常營運。

・備援計畫

設置妥善的備援機制，將可在復原時間目標（RTO）內恢復系統運作。

・持續運作計畫

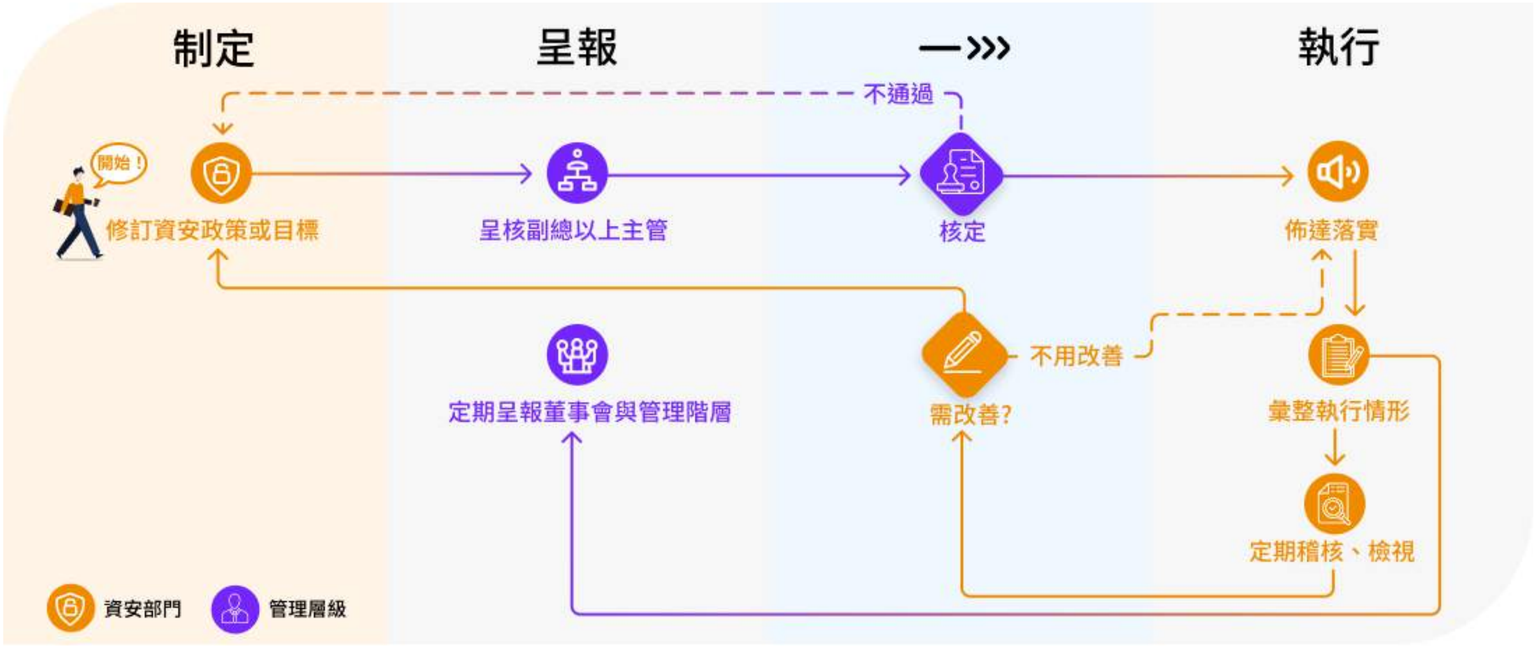
制定持續運作計畫，定期辦理災害演練，降低核心業務與系統無法持續運作的風險。

持續精進

即使做好了事前預防、事中偵測以及事後應變，大多公司也有已設置多年的資安設備與流程，可駭客的攻擊手法多變，不論是最低限度或完善的資通安全管理，已然成形的資安策略及措施是否符合現今需求且有效防禦威脅，皆需要藉由資產盤點、定期稽核與風險評估，確認資產等級、風險衝擊值對企業的影響。

另外，資安事件發生時也是企業學習、精進的機會，透過解析、辨識攻擊行為與手法，再回過頭來檢視資安策略是否還有不足之處，以改善資安措施與防禦策略。透過不斷學習和改進，企業可以保持高度的資安韌性，未來發生資安事件時能夠快速而有效地應對威脅。

故建議製造業客戶定期執行下列流程，方可持續精進：



全場域聯防以利企業永續經營

資安事件頻頻爆發，受到波及的企業無不損失慘重，好不容易建立起來的商譽也難以彌補，為了提升全國整體資安防護力，金管會於 2021 年底發布了「上市上櫃公司資通安全管控指引」，給予企業資安的落實方向，鼎新也提醒企業務必檢視法規合規度，切勿以身試法，未來全球各國的資通安全相關法規將會更加嚴謹，以守衛國家及人民的財產安全。

OT 資安看重資安要素 CIA 的順序不同

一個都不放過－跨場域、跨品牌、跨方案

資安三要素中的可用性（Availability）被製造業奉為圭臬，所以工控場域間的串聯極為重要，萬萬不可因為銜接不利而影響運營。企業資安也一樣，不僅需要全場域聯防，連接品牌眾多、規格不一的產品時，也要考量是否能夠透過技術整合，用統一的標準管控場域資安，讓不同的資安方案有效協作，共防外敵。

當國際情勢與資通安全息息相關，駭客通常跨國而來尋覓看似容易下手的肥羊，製造業也要具備「跨」彈性，才能將主控權掌握在自己手裡，不放過任何一個有機會造成威脅的風險。

找到平衡支點－數位轉型兼顧穩定運營

為提升競爭力，包含製造業在內的各大產業都在嘗試數位轉型，尤其智慧工廠、智慧製造皆是時下最夯的議題，顯現了自動化效益已無法滿足市場需求，企業無不期望透過數位轉型促成業績、營收更上一層樓。數位轉型的新思維讓製造業從傳統保守邁向時代潮流，必經歷程便是數位化以及導入應用工具，使企業可騰出更多心力專注於核心業務，然而除了運用新概念、新工具協助企業降本提效外，更要留意如何兼顧資安，確保數位轉型之下的企業依舊具備堅實可靠的安全性，利於企業能量生生不息、永續發展。

鼎新電腦站在合作夥伴的角度，協助製造業客戶完善企業運營，發現多數企業對於資安的重視程度雖已提升，但仍困在過往的既有觀念中，認為資安只是在花錢防禦可能並不存在的敵人。興許是因為其帶來的衝擊不外乎營運中斷或資料外洩、勒索贖金，無法事先量化損失，看不見的數字讓人不痛不癢，更何況每個人、每家企業都會遭遇到資安攻擊的機率看似並不大。

但台灣已將資通安全防護拉高至國安層級，建置有效信任的資安策略與措施不僅是企業的法定責任，還可替公司降低潛在風險及其後損失，保護歸類於無形資產的品牌聲譽，提升客戶滿意度以建立良好的客戶關係，有助於企業長期穩健發展，永續經營。

參考資料

Fortinet《2023 上半年全球資安威脅報告》：
https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-1h-2023.pdf

趨勢科技 Trend Micro《工業網路資安現況：IT 與 OT 人員、流程及技術的匯流》：
https://resources.trendmicro.com/Industrial-Cybersecurity-WP.html

趨勢科技 Trend Micro《ICS 與 OT 網路攻擊趨勢》：
https://www.trendmicro.com/zh_tw/research/22/h/ics---ot-cybersecurity-attack-trends.html

CIO Taiwan《2022 年美國版 CIO 大調查報告》：
https://www.cio.com.tw/american-cio-report/

CIO Taiwan《2023 年 CIO 大調查報告》：
https://www.cio.com.tw/events/ciosurvey-2023/

Fortinet《2023 年 OT 與網路資安現況調查報告》：

https://www.fortinet.com/tw/demand/gated/report-state-ot-cybersecurity

洛克威爾自動化《工業營運的 100+ 網路資安事件剖析》：
https://www.rockwellautomation.com/en-us/campaigns/cyentiareport.htm

行政院國家資通安全會報技術服務中心《資安威脅趨勢及防護策略》：
https://secutechinfosecurity.tw.messefrankfurt.com/content/dam/messefrankfurt-redaktion/infosecurity/2021-march-seminar-agenda/ 資安威脅趨勢及防護策略 _ 行政院國家資通安全會報中心 - 吳啟文 - 主任 .pdf

鼎新電腦 × 天下實驗室 CommonWealth Lab

專家解析AI 如何加速企業轉型？

生成式AI技術將帶來第三波資訊革命！

想要在這一波變革中脫穎而出，企業不僅反應要快，例如協助員工熟悉這一波變革跟進行相應的組織調整等，也得要開始訓練自己的企業（人工智慧）大腦。

同時，將數據驅動的智能決策模式融為企業文化與員工DNA，一步一腳印擴大應用範疇，為企業打造超級大腦與員工智慧助理等應用，以數智企業之姿，開創新藍海市場！

掃瞄下載

全新未來工作模式 67頁全收錄

▶▶數智轉型白皮書

專家如何看數智企業樣貌

微軟全球合作夥伴 解決方案事業群 陳仲儒

在 A(人工智慧) B(巨量資料) C(雲端)等數位科技的加持下，未來企業不僅能更好賦能員工、優化營運流程(營運韌性)、重塑商品與服務模式，還可以體驗優化等方式深化跟客戶的互動關係。

波士頓顧問公司董事總經理 暨資深合夥人 徐瑞廷

未來企業應該是一個可以健康成長、穩健獲利且聰明用錢的公司，透過轉型為數智企業，勝局將會提升、成為未來贏家。

ikala 共同創辦人 暨執行長程世嘉

在生成式人工智慧技術的帶動下，不僅員工的生產力會比現在提升40%到50%，企業營運模式也會大量倚靠人機協作，此外，可以眞正的將企業累積的數據資料轉換為新黑金。

Follow Us

更多行業知識

鼎新電腦
官方網頁

鼎新電腦
LINE

就享知
就想知道的數位知識

鼎新電腦股份有限公司
Data Systems Consulting Co., Ltd.

鼎捷軟件·鼎捷軟件(越南)·鼎捷軟件(馬來西亞)·鼎捷軟件(泰國)·鼎華智能·智互聯·鼎捷移動

▸客戶服務專線 :0800-888-162