

# 台灣工具機暨零組件工業同業公會

## 工具機產業資安藍圖評估報告



【計畫執行單位】：台灣工具機暨零組件工業同業公會

【產業輔導單位】：財團法人工業技術研究院

【資安輔導單位】：勤業眾信聯合會計師事務所

中華民國 111 年 11 月 15 日

## 工具機產業資安發展藍圖策略

產業願景	2030年工具機產業發展願景		
	提升工具機產業對國家關鍵製造業發展貢獻、促進工具機產業高值化、提升台灣全球工具機產業影響力		
資安願景	中期發展目標~2025年	長期發展目標~2030年	
	台灣工具機產值全球占比達到6%；台灣工具機出口金額全球占比達到8%；車床、加工中心機出口單價增加。工具機整機廠商附加價值率(折舊)提升..	台灣工具機產值全球占比達到8%；台灣工具機出口金額全球占比達到10%；車床、加工中心機出口單價增加；工具機整機廠商附加價值率提升...	
	短期目標~2022年	中期目標~2025年	長期目標~2030年
	<ul style="list-style-type: none"><li>• 建立產業資安推動小組</li><li>• 建立產業專屬資安成熟度評估報告(13家企業)</li><li>• 規劃產業資安藍圖</li></ul>	<ul style="list-style-type: none"><li>• 擴大資安成熟度，協助廠商<b>策略性規畫提升資安能量</b></li><li>• 建立工具機<b>產業資安指南</b></li><li>• 建置工具機產業「資安檢測服務」及「資安緊急應變服務」等資安諮詢服務。</li></ul>	<ul style="list-style-type: none"><li>• 推動工具機產業資安交流座談會(分享攻擊趨勢、供應鏈資安趨勢、應對策略分享)</li><li>• 推動工具機產業共享資源(教育訓練、資安諮詢、聯合監控及分析中心等)</li></ul>

## 一、產業資安藍圖

### (一) 台灣工具機暨零組件工業同業公會的資安急迫性：

工具機產業為台灣產業非常重要一個環節，在台灣機械工具發展有重要貢獻，不僅供給台灣內部之製造生產需求，亦外銷於海外，為全球前幾大工具機生產國，尤其在車床與銑床等，因此，工具機企業之持續營運為各組織所重視之關鍵重點，然而若遭受資訊安全攻擊，則可能會導致營運衝擊，嚴重更可能造成商業機密外洩，後果不容小覷。

透過執行此次專案，了解到台灣工具機暨零組件工業同業公會之參與企業現況，目前大部分組織尚無使用系統性的方式導入資訊安全管理系統來管控企業內資訊安全，但

部分企業針對存取控制、營運持續已有陸續進行控管，也欲針對資料保護、當前弱點評估進行加強，因此，各組織短期目標得以先著重於評估自身資訊安全控管之現況，並接續分析組織可能遭受之威脅，以擬定對應之應對措施。

## (二) 台灣工具機暨零組件工業同業公會的資安中期目標：

### 1. 擴大資安成熟度，協助企業策略性規畫提升資安能量

協助企業檢視整體資訊系統既有控制措施之完整性與妥適性，並檢出潛在資安威脅與弱點。

除此之外，經持續蒐集資安威脅情資，除了得以提供企業檢視內部控制狀況，也得以進行內部宣導，更可以了解全球資安實際威脅趨勢，提升台灣工具機暨零組件工業同業公會企業同仁資訊安全意識；針對資安相關技術/管理證照，皆可以鼓勵同仁進行考取，以提升組織內部之資安能量，以及提升遭遇資安事件之反應速度與能力。

經檢視整體資訊系統既有控制措施之完整性與妥適性，並透過提升內部資安能量，即可以評估優先順序依序完成改善，進而提升整體之資安成熟度。

### 2. 建立工具機產業資安指南

參考現行之國際標準，並鼓勵組織建置資訊安全管理制度，針對資訊安全管理體系、政策、組織、資產、系統開發、供應商關係、資安事件、營運持續等進行管理及訂定組織資安政策文件，建立以計畫-執行-檢查-行動(Plan-Do-Check-Act, PDCA)為基礎之管理制度，可參考資訊安全相關標準如：ISO 27001 資訊安全管理系統

(Information Security Management System, ISMS) 標準、IEC 62443 工業自動化及控制系統安全標準等。

並經由研析工具機產業之常見攻擊事件，針對工具機產業中風險較大且需要注意之威脅環節進行資料彙集並予以分類。

最後，透過結合國際安全標準與世界資安威脅趨勢，即可建立起工具機產業之資安指南，並依照趨勢與產業現況不斷進行適應性調整，即可符合工具機產業之資安需求，也可以協助各企業了解產業資安現況。

### 3. 資安檢測服務、資安緊急應變服務等資安諮詢服務

台灣工具機暨零組件工業同業公會得以鼓勵/協助企業透過資訊資產盤點，針對網路環境、提供對外服務資訊系統、伺服器主機、工業控制系統、端末設備等，進行相關資訊安全管控措施之評估，以檢視組織整體資訊安全架構、相關安控機制及防禦程度；亦得以鼓勵/協助各企業進行企業整體網路安全風險評估並規劃符合本身企業文化的資安長及資安專責單位的架構。

從網路架構安全設計層面、外部網路威脅層面、系統安全設定層面、模擬駭客攻擊層面，抑或是實際檢測企業內部網路是否已遭惡意入侵，其一系列完整之資安健檢，搭配資安緊急應變演練服務，不僅可協助發現企業潛藏的資安危機，並得以使企業儘早因應、對症下藥，以最有效益的方式，降低資安風險。

### (三) 台灣工具機暨零組件工業同業公會的資安長期強化方向：

1. 推動工具機產業資安交流座談會(分享攻擊趨勢、供應鏈資安趨勢、應對策略分享)

台灣工具機暨零組件工業同業公會得以將日常蒐集之資訊安全情資進行趨勢之分享，並規劃資安人員相關教育訓練，使得公會中之企業資安人員可以發揮所長於企業。

## 2. 推動工具機產業共享資源(教育訓練、資安諮詢、連合監控及分析中心等)

針對台灣工具機暨零組件工業同業公會中，欲進行資訊安全能量提升之企業，得以組成一個工具機產業資訊安全小組，定期進行資訊安全分享與討論，了解產業內資安趨勢，甚至可以運用企業分工之方式減少各企業投入成本，進而可以平衡投入成本，亦可以提升企業之資安能量。

本資安藍圖評估報告乃受台灣工具機暨零組件工業同業公會(以下皆簡稱「TMBA」)之委託，並根據工業技術研究院之企業資安評級工具之資安成熟度框架，參考企業自我評估之結果，並執行資訊安全評估訪談作業後所產製之報告。勤業眾信聯合會計師事務所(以下簡稱「勤業眾信」或「本所」)之責任為以獨立第三方之角色評估台灣工具機暨零組件工業同業公會中參與之 12 家企業，包含目前既有控制措施之完整性與妥適性，進而發現潛在的資通安全威脅與弱點，提供企業強化其網路與資訊系統安全防護能力之建議。本資安藍圖評估報告(及其附件)僅供台灣工具機暨零組件工業同業公會及相關主管機關作為監理之參考，非經本所及台灣工具機暨零組件工業同業公會雙方同意，不可作為其他用途或分送其他人士。