資安領導者取得認證成趨勢

借重美國國防部 CMMC 推動數位安全轉型

資安市場重要的屬性是「信任」，創辦人或技術領導者若能具備相當實力的資安專業知識，則更增加信任度。其中，伊諾瓦總經理萬述寧除了有資安技術最高桂冠 CISSP 外，近兩年更投入 CMMC 領域，取得 CCA、CCP 等資格。

採訪／施鑫澤　文／林裕洋

在資安等於國安的浪潮下，資訊安全已不僅是 IT 部門的工作，而是關係到國家安全、企業存續的戰略性議題。面對日趨複雜而多變的網路安全威脅和法規要求，企業領導者必須具備超越技術層次的宏觀視野、思維與作為。

伊諾瓦（ENOVA）總經理萬述寧認為，資安領導者最重要、最具戰略性的任務，是全面性地建制**安全企業架構（Security Enterprise Architecture）**並建構**系統安全架構（System Security Architecture）**用以服務商業程序，由上至下驅動，讓安全元素及要件融入公司整體治理，經由制度化的每日實踐型塑資安文化，進而促進資安成熟度。

他強調，最重要的關鍵在於**由上至下驅動**，因為只有領導者才能根據其對業務摸式或程序的了解制定目標、擬定政策、充分授權並編列充裕預算。資訊安全部門存在的意義在於服務企業業務、各部門、外部客戶與供應鏈，因此，它是專業服務，可考慮獨立預算及營運模式，例如，轉變成利潤中心制。

萬述寧表示，一套完整資安戰略必須思考**縱深防禦（Defense In Depth）**，依照**機密性、完整性和可用性（CIA）**三大安全目標進行精確的資訊與資訊系統風險評估。NIST 根據美國聯邦法案 FISMA 制定的 FIPS 199 標準指出，資訊與資訊系統 CIA 必須分別評估為各有詳盡定義的三級風險：Low、Moderate 與 High，並以資訊風險為主要決定點，採取高水位線；意即當資訊與運行該資訊的資訊系統中有 CIA 任一項風險被評估為「High」，那麼整個資訊系統資產就被歸類為高危險資產。

因此，高危險資產，如負責線上訂單的資料庫伺服器等，資安主管就必須著手思考強化與改善方式，以 FIPS 200 標準入門，參考最新版 NIST SP800-53 標準，根據風險評估結果客製化控制方法用以達成**適度安全（Adequate Security）**目標。即使駭客攻破第一道防線，還有第二道、第三道防線，藉由層層設防方式降低損失。

然而令人遺憾之處，在於現今多數台灣企業的弱點評估機制，仍停留在弱點掃描層面，且**缺少能判斷弱點實質影響的安全分析專家**。缺乏系統安全架構全盤思慮，使得資安改善受限於孤立式運作，無從了解該改善對資訊系統及其服務商業程序上下游安全性影響。

因此，企業若要提升整體資安，必須從領導層開始，積極學習和掌握國際級的標準與治理精神，培養安全評估分析人才，將資安從技術需求提升為企業的核心文化和戰略韌性。

學習資安七層安全架構 物理層到應用層的思維轉變

成立於 2000 年的伊諾瓦，擁有專業資訊系

伊諾瓦（ENOVA）總經理萬述寧。

統安全和加密晶片工程專業知識，專注於開發即時加密晶片 ASIC 及資料安全解決方案，以滿足對傳輸中資料（雲端或點對點）和靜態資料（儲存）安全性日益增長的需求，並提供物理層級抗量子（Quantum Resistant）晶片、身份驗證（Identity-based Authentication）、安全啟動（Secure Boot）、信任根（Root of Trust）等資通安全解方。憑藉著廿多年的資訊安全經驗，該公司提供 **FIPS 140-2 (3) 級認證的單晶片加密模組**和系統級別的安全解決方案，目前擁有超過 15 項全球發明專利。

除此之外，伊諾瓦在國際安全驗證方面擁有豐富的經驗，包括 **FIPS 140-2(3)、Commercial Solution for Classified（CSfC）和共同準則（CC；Common Criteria）**。該公司晶片產品和解決方案被廣泛採用，涵蓋航空航太、國防、軍事、政府、企業、工業和博弈等客戶。對於專業消費者客戶，該公司提供 **Enigma Pathway** 系列硬體加密器，能加密任何可偵測得到的儲存硬碟（包括 NAS 和雲端硬碟）上的靜態資料，以及傳輸中的資料。

萬述寧指出，我們是從安全晶片起家，只是在與客戶溝通時發現，彼此對資安思維存在很大差距。企業在討論網路安全時，通常是聚焦在網路架構第七層的應用層，如何進行識別、驗證、存取控制，或是部署 WAF（Web Application Firewall）等，與我們熟悉的**物理層控制**差距太遠，也形成溝通上的困擾。

為此，萬述寧決定去學習整個「資安七層安全設計」，**CISSP（Certified Information Systems Security Professional）課程**涵蓋了網路通訊的七層安全設計，從應用層一路往下到物理層，每個層級都詳細說明與安全相關的部分。當然，最後他也考取 CISSP 認證。為此萬述寧透露，取得 CISSP 認證能清楚瞭解客戶在應用層上的各種需求，且能用共通語言向客戶介紹伊諾瓦的安全晶片定位、可解決哪些問題，以及與應用層資安方案有哪些不同之處，這對於了解客戶痛點與市場趨勢帶來極大幫助。

物理層彌補應用層缺點 有效改善資安防護機制

萬述寧認為，相對於應用層的安全挑戰，**物理層安全**具有巨大的相對優勢。因為，一個計算機裝置的基本組成單元為中央處理器、記憶體、軟韌體與作業系統，將它們的安全問題包括認證、存取控制、基本組態、弱點、資訊機密性及完整性處理好了，在物理層建立好「安全內核」進而形成**可信任計算基礎（Trusted Computing Base）**，即可大量減少其它層可能發生的安全疑慮。

一個缺乏機密性與完整性的韌體可被惡意程式任意置換用以遠端遙控或洩露機敏資訊，或參與 DDoS 分佈式阻斷服務攻擊而不自知；或者，缺乏安全組態的作業系統無法防護 DoS 阻斷服務和惡意程式攻擊；又或者，缺乏安全組態的 CPU 可被惡意程式以資料溢位（Buffer Overflow）攻擊而造成資訊外洩或程式崩潰；又或者，缺乏即時對記憶體／儲存裝置加密能力而遺失、遭竊或間諜行為洩露機敏資訊等。

因此，應用層的軟體在一個缺乏安全組態的作業系統上運行，其負面結果可預期。反之，在可信任計算基礎上運作的應用層軟體只須考量本身是否已

在 DevOps 流程開始時的 Requirement Gathering 階段加入安全元素與要件並驗證之即可達成適度資訊安全設計。

「伊諾瓦的安全晶片可在物理層提供絕佳保護，能強化前述提到的各種計算機裝置的基本組成單元，讓應用程式在一個安全架構上運行。」萬述寧解釋：「此種從底層出發的資安設計概念，也就是「Security by Design」，在產品開發設計階段即融入資訊安全要件，讓產品形象效益更突出、更容易向客戶和夥伴解釋，自然也有助於產品銷售。」

落實 CMMC 建構資安文化與資訊治理政策

CMMC（Cybersecurity Maturity Model Certification）網路安全成熟度模型認證是由 Laws 法律（FISMA、E.O. 13556），32 CFR Part 170及48 CFR Part 204 法規則秉承法律要義，明定規則及實施辦法；根據 CFR 制定的政策執行、實施與檢核標準，為**美國戰爭部（DoW；Department of War）**主導推動立法的網路資安標準框架，主要目的是確保參與**美國國防供應鏈（DIB；Defense Industrial Base）**的承包商，能夠符合一定的資安防護水準，保護敏感 **Federal Contract Information（FCI）聯邦合約資訊**與 **Controlled Unclassified Information（CUI）受控非機密分類資訊**不被竊取或外洩。其位階分明，環環相扣，是一部難能可貴的資訊安全治理標準。

■ CMMC 專注於由上至下驅動的資料治理

CMMC 要求國防供應鏈建構系統安全架構並撰寫**系統資訊安全計畫（System Security Plan, SSP）**用以服務商業程序，**由上至下驅動（Top-down Driven）**，設計護欄（Guardrails）用以保護整體生態系，讓安全元素及要件融入公司整體治理，經由制度化的每日實踐過程型塑資安文化，進而促進資安成熟度。

■ CMMC 的護欄（Guardrails）

CMMC 設計有三個護欄。**其一為嚴謹的控制方式論述、評估標的、方法及程序**，比對起 ISO 27001 抽象描述，CMMC 是一套非常精準且能有效提升企業資訊安全的標準，適合實作。

其二是嚴格要求行為準則（Code of Professional Conduct；CoPC）、道德和利益衝突條款（Conflict of Interest；COI）。其三是美國聯邦「假聲明法」（False Claims Act）搭配吹哨者條款（Whistle Blower），在評估過程中蓄意欺騙聯邦政府或作假會面臨嚴重的賠償條款。

萬述寧指出，CMMC 精髓並不在於技術細節多厲害，而是在於**強調道德與公正**，這也真正展現資安治理的高度。此標準要求評估人員必須遵守高度的道德和利益衝突迴避之要求。

例如，身為 **CCP（CMMC Certified Professional）**或 **CCA（Certified CMMC Assessor）**不能對自己提供過顧問服務的公司進行評估，也不能評估其親屬任職於資安重要職位的公司。

台灣適合推動 CMMC 嗎？

臺灣普遍認為 CMMC 只是「美國國防供應鏈」標準，推動力道仍然太小且方法不正確，事倍功半。但是，台灣真的適合嗎？

首先，不論是否為美國國防供應鏈，CMMC 都是一部優秀可實踐的資安治理標準。它教的方法若稍做變化即可擔當我國國家資安標準。其次，CMMC 實踐 FISMA 目標，專注治理聯邦政府資訊與資訊系統安全。其擷取 NIST SP800-53 精髓，客製化 Moderate Controls 形成 **NIST SP800-171R2** 用來保護非聯邦政府資訊與資訊系統。最後，類似於 FCI／CUI 每家企業都有，方便重新定義。

萬述寧建議，資安主管必須調整資安策略的出發點，絕非是「想節省成本」，而應該是以服務商業程序為中心思考「建制系統安全架構」，由上至下驅動，讓安全元素及要件融入公司整體治理，經由制度化的每日實踐型塑資安文化，進而促進資安成熟度。

其中，最重要的關鍵在於**由上至下驅動**，因為只有領導者才能根據其對公司治理、業務模式或程序的了解制定目標、擬定政策、充分授權並編列充裕預算。