人工智慧如何影響網路安全和安全管理?

隨著人工智慧帶來的好處，例如提高生產力、降低營運成本和加快產品上市速度等，越來越多企業正在廣泛應用人工智慧。在新冠病毒疫情期間，人工智慧的採用率上升，某間全球決策情報公司在 2021 年對 5,000 多家企業進行一項全球調查結果顯示，43%的企業報告指出，由於新冠病毒疫情，他們的公司加速推出人工智慧。

其次，雲端服務加速人工智慧的採用。Tractica 預測，到 2025 年，人工智慧在公有雲服務總收入中的占比將高達 50%。該研究公司還預計，全球人工智慧市場收入將以每年 57%的速度成長。另外，O'Reilly 於 2021 年對全球 3,000 多名參與者進行調查顯示，人工智慧應用第二重要的產業是科技、金融和醫療保健行業。

企業在大規模應用人工智慧的同時，仍普遍存在若干憂慮，其中包括人工智慧的安全性和合規性。

挑戰與風險

人工智慧市場的成長並非一帆風順，意外事故頻繁發生，例如在不知情或未經同意的情況下獲取大約 160 萬個人的機密醫療紀錄而面臨訴訟、自動駕駛車禍等人身傷害事件、人工智慧聊天機器人被平臺上的不當發文破壞而在推出後不到 24 小時內開始發布攻擊性推文等事件。從這些案例中可以看到採用人工智慧帶來的資料隱私和安全隱患，以及人工智慧的漏洞，所以採用人工智慧有相對應的挑戰和風險。

採用人工智慧技術時常見的挑戰包括：

- 用於訓練人工智慧的敏感資料可能會引發隱私問題，尤其是在涉及個人資料的情況下，且資料可能會在沒有足夠安全保護的情況下受到損害
- 訓練數據中的偏差會影響人工智慧的行為或結果，導致解決方案無法按預期運行
- 人工智慧系統錯誤可能對用戶造成傷害
- 人工智慧使用的算法和生成的結果是否可以被專家和用戶理解和解釋
- 誰對人工智慧做出的決定以及人工智慧的運作方式負責
- 人工智慧是否符合道德、社會規範以及企業價值觀
- 缺乏開發或監督人工智慧模型，並對人工智慧進行管理的專業人才

使用人工智慧時會涉及的風險包括：

- 營運風險：人工智慧能否實現業務目標，以及人工智慧失敗時是否有應急方案
- 技術風險：在人工智慧開發過程中，與使用不同技術相關的風險
- 模型風險：與人工智慧模型可靠性相關的風險
- 第三方風險：第三方參與人工智慧開發過程時的相關風險
- 安全風險：與支持人工智慧系統的數據、軟體和硬體相關的資訊安全和網路安全風險
- 道德和法遵風險
- 與訓練數據相關的數據品質風險

監理要求

隨著人工智慧技術的應用和發展，監理機關已經發布若干與人工智慧安全相關的監管要求或指南。同時，亦有不同監理機關正在起草和發布更多法規和標準。例如：

- 《人工智慧法》（Artificial Intelligence Act）（草案）
  - 歐盟執委會於 2021 年 4 月 21 日提出法規草案，並具有域外效力
  - 法規規定的某些義務包括風險管理、資料治理、技術文件、紀錄保存、透明性和向使用者揭露資訊、人為監督、準確性和網路安全穩健性

- 《國家人工智慧創新法案》（National AI Initiative Act）
  - 美國國會於 2021 年 1 月頒布的一個國家層級總體框架，以加強和協調美國所有部門和機構的人工智慧研究、開發、示範和教育活動

- 香港金融管理局（HKMA）發出的通函
  - 香港金管局的「人工智慧高級原則」通函為銀行業使用人工智慧應用程式提供原則和指導
  - 香港金管局的「授權機構在使用大數據分析和人工智慧方面保護消費者」通函，就銀行業使用大數據分析和人工智慧的消費者保護方面提供了一些指導原則

- 中國《國家新一代人工智慧標準體系建設指南》
  - 於 2020 年發布，《國家新一代人工智慧標準體系建設指南》概述建立人工智慧國家層級標準體系的策略，涵蓋人工智慧不同方面的標準，如硬體和軟體、概念、應用、安全和倫理
  - 預計 2023 年會初步完成人工智慧標準體系

以上監管/指南共同提出的控制要求包括：

- 透明性：在提供服務之前，應告知使用者該服務所採取的人工智慧技術以及所涉及的風險
- 可解釋性：應當向所有相關方解釋應用程式的邏輯
- 隱私和資料治理：遵守適用的資料保護要求，並確保用於訓練人工智慧應用程式的數據具有良好的品質和相關性
- 公平：人工智慧決策不會歧視或表現出對任何使用者族群的偏見
- 可靠性、彈性和穩健性：確保人工智慧決策的準確性，並實施有效的網路安全措施，以因應對人工智慧模型和應用程式的攻擊
- 問責制：確保對人工智慧相關的決策建立問責制
- 人工代理和監督：實施應急措施，在人工智慧出現意外事件時允許人工干預

治理人工智慧的運用

Gartner 預計，到 2026 年，有實施人工智慧透明性、信任和安全性的組織將看到他們的人工智慧模型在採用、業務目標和用戶接受度方面達到 50%的成果改進。Gartner 調查結果顯示，組織已經部署許多 IT 領導者無法解釋的人工智慧模型，缺乏知識和理解可能會產生嚴重的後果，當依賴增加時，人工智慧模型表現不佳的影響會被放大。不管理人工智慧風險的組織更有可能遇到負面的人工智慧結果和違規行為。模型不會按預期運行，並且會出現安全和隱私問題、財務和聲譽損失以及對個人的傷害。錯誤執行人工智慧也可能導致組織做出糟糕的業務決策。

為確保人工智慧系統的安全性和合規性，企業應當對人工智慧技術的運用進行治理。有效的人工智慧治理將包括以下關鍵控制領域：

- 法規和政策：瞭解適用的法律和法規，制定人工智慧領域的政策
- 標準和規範：制定人工智慧安全要求的標準和規範，以納入人工智慧系統和解決方案
- 技術方法：實施技術措施以因應人工智慧風險
- 安全評估：評估人工智慧系統的安全性、彈性和穩健性，並進行持續監控和審查
- 人才發展：為負責人工智慧開發、部署和管理的員工提供充分的培訓
- 可控環境：確保人工智慧解決方案在其整個生命週期內可解釋且一致，並維持人為對人工智慧系統的監督

安全管理正面臨的挑戰

首先，網路安全產業的勞動力缺口正逐年擴大。在需求面，因新冠病毒疫情肆虐下，世界各國為此實施不同程度的防疫政策，保障人民生命健康。為因應經商環境的轉變，愈來愈多企業因此走向數位化轉型，包括將線下業務移至線上發展、安排員工遠距工作、把 IT 基礎設施遷移到雲端運算環境等，力求在激烈變化的環境下為企業獲取新的業務機會。但與此同時，企業在網路安全方面所暴露的攻擊面亦隨之增加。為此，企業需要採取措施加強網路安全防護水準，例如聘用網路安全專家或尋求安全託管服務來為企業部署安全解決方案，並對企業 IT 環境進行監控、評估和優化。

其次，在安全服務供應方面，有研究報告指出可以看到安全營運中心（SOC）在日常營運當中存在不少痛點，有 73%的受訪者認為「不斷增加的工作量會導致工作上的倦怠」，有 65%的受訪者表示「那些痛點令他們考慮辭去分析師崗位以謀求其他職位」，從長遠的角度來說，市場必將出現安全分析師供應短缺的情況。不少 SOC 的安全分析師長期面臨著大量枯燥的工作，例如長時間輪班、警報帶來的乏味、耗時的調查，因此，有部分經驗豐富的分析師願意轉向其他職務以減少工作壓力。此外，安全營運團隊每天都需要處理來自多個安全平臺的警報，其中包括不少虛假警報，這遠遠超出了團隊人員能夠負擔的處理速度。

最後，隨著網際網路應用的普及化，相對應網路威脅隨之上升，而且其複雜性也相對增加，為此對網路安全也帶來挑戰。如今，行動設備、物聯網、雲端運算在企業中的應用日益普及，攻擊面也相對增加。此外，駭客可以利用人工智慧來不斷變形病毒/惡意軟體，而傳統的靜態防禦解決方案未必能對此有效檢測以及阻斷。另一個原因是網路犯罪即服務（Cyberattack-as-a-Service）令網路攻擊變得普及，攻擊者自身不須擁有強大的駭客知識，亦可以透過支付加密貨幣獲得攻擊工具。

人工智慧如何改變安全營運

人工智慧在安全營運中的其中一大作用是協助安全分析師工作，畢竟，它不太可能完全取代有經驗的人類。反之，人工智慧可以專注於比人類擅長的領域去協助人類，如分析大數據，替人類進行繁瑣、重複的任務，以便分析師能夠發揮更複雜的技能，如創造力、細微差別和專業知識。

此外，透過人工智慧對安全事件進行分析，查詢大量資料並在整個網路中進行檢視，以蒐集事件的背景並進行調查，整理出優先順序高的事件讓分析師加以關注。同時，人工智慧透過分析人類分析師調查警報的過程，進行訓練以及機器學習，當未來有類似的事件發生時，機器可在通知分析師前生成多個查詢，並同時調查所有威脅。

人工智慧在安全營運的應用

支援人為作業

為因應大量的警告以及進階持續性滲透攻擊（Advanced Persistent Threat，APT），網路安全營運團隊積極尋求人工智慧和機器學習來提高效率，分析師因此能減少分析所需時間，包括採用人工智慧的威脅獵捕工具（Threat Hunting Tool）提高企業對隱藏威脅的檢測。例如，採用無監督機器學習算法的使用者行為分析工具（User Behavior Analytics，UBA）可以持續監測和分析使用者活動、系統安全變化、網路流量和對應用程式和資料的存取進行檢測和標記異常情況，使得該威脅對環境造成破壞之前，企業可以把未知的威脅更快地轉化為已知的威脅。因此，網路安全營運團隊在人工智慧和機器學習工具協助下，可以採取更積極的策略，對事件做出相對應的反應。

識別攻擊

針對惡意軟體以及惡意行為，傳統的安全解決方案大多以特徵比對（Signature-Based）檢測來進行識別。可是，它必須在漏洞被公開以及廠商開發團隊加入攻擊特徵後才能識別威脅。然而，時下較流行的攻擊大多以駭客攻擊戰術流程 TTP（Tactic, Technique, Procedure）去避開特徵的檢測，採用人工智慧檢測，可透過分析大量日誌、事件類型以及結果去識別全新、經過變形或 APT 攻擊，從而更快識別出威脅。

事件回應自動化

在資安事件回應（Incident Response）方面，相對於安全分析師，人工智慧安全工具一旦發現威脅就可以對其做出反應。事件回應自動化使事件的反應更加容易，速度和效率更高。其次，人工智慧和機器學習在資安事件回應中透過記錄威脅模式及其隨時間變化的特徵，建立威脅資料庫並分析這些威脅如何運作，從而根據分析來建立資安事件回應預案。

透過使用由人工智慧和機器學習驅動自動生成的應急處置方案，可以使 SOC 更有效地集中資源。人工智慧事件回應工具可以根據風險分析和以前的事件回應，當面對類似的安全事件時，建議分析師如何執行。人工智慧事件回應工具亦可根據安全分析師的專業知識、實際可用性和案例歷史，做出資源分配，向 SOC 團隊提供建議。這有助於提高整個團隊的分析效率，同時利用自動化來節省安全分析師的時間，以進行更具附加價值的工作。

網路安全營運團隊該如何面對人工智慧

透過以上對人工智慧影響安全營運的瞭解，我們可以預見人工智慧的出現將改變大多數 IT 和資訊安全行業人員的角色。有部分的行業人員對此有著極大的擔憂，例如擔心自己會被人工智慧控制的機器人取代。事實上，人工智慧工具能為資訊安全專業人員創造機會，使他們能夠更有效地履行工作職責，同時也可利用新的洞察發現來改善整個資訊安全計畫，並與 SOC 之外的其他團隊展開更多合作。

在一般的 SOC 工作中，安全分析師每天查看網路流量和來自不同系統的日誌，以確定安全事件是否構成需要進一步調查的威脅。而 SOC 傳統的分工上，一階（Tier-1）分析師負責查看警報，二階（Tier-2）分析師尋找可能的攻擊，三階（Tier-3）分析師執行事件回應，安全工程師則負責想出更好的方法來使基礎設施更加安全。

然而，當我們把人工智慧以及自動化應用在安全營運的場景後，人工智慧會代替分析師處理以往相對低階和繁雜的日常工作，如查看警告、分析、檢測等。因此，團隊必須調整每個職務角色以及職責，調整培訓計畫的重點，例如讓分析師建立與人工智慧系統合作的技能，建立良好的溝通技巧以便對企業的業務部門解釋安全問題。

結語

在當今人工智慧持續發展的趨勢下，企業應以不同視角去看待人工智慧的使用，特別是人工智慧如何影響網路安全管理。雖然人工智慧的使用為企業帶來挑戰和風險，但同時人工智慧也能有效解決勞動力短缺以及有效提升網路安全管理的效果和效率。企業為有效因應挑戰以及控制風險，應及早制定內部人工智慧安全要求的政策、標準和規範，對人工智慧的應用進行研發，建構人工智慧驅動的網路安全管理能力。在企業不斷發展的道路上，人工智慧將協助企業在現今的大環境中提高生產力及綜合競爭力。

最後，安永專業團隊希望透過提供各種服務，協助企業在評估、計畫、建構、實施等不同階段，成功執行人工智慧網路安全和安全管理。服務包括但不限於：

- 合規性評估
- 安全風險評估
- 內部政策的制定和審查
- 員工培訓教材和研討會
- 人工智慧安全營運工具的調整和實施
- 人工智慧安全營運工具成熟度評估

聯繫安永

張騰龍
總經理
安永諮詢服務股份有限公司
+886 2 2757 8888 ext. 88863
Tony.Chang@tw.ey.com

黃昶勳
總經理
安永企業管理諮詢服務股份有限公司
+886 2 2757 8888 ext. 88862
Jon.Huang@tw.ey.com

安永 | 建設更美好的商業世界

安永的宗旨是致力建設更美好的商業世界。我們以創造客戶、利害關係人及社會各界的永續性成長為目標，並協助全球各地資本市場和經濟體建立信任和信心。

以數據及科技為核心技術，安永全球的優質團隊涵蓋 150 多個國家的業務，透過審計服務建立客戶的信任，支持企業成長、轉型並達到營運目標。

透過專業領域的服務 - 審計、諮詢、法律、稅務和策略與交易諮詢，安永的專業團隊提出更具啟發性的問題，為當前最迫切的挑戰，提出質疑，並推出嶄新的解決方案。

加入安永 LINE@好友

掃描二維碼，獲取最新資訊。

APAC No. 14007109
ED None

ey.com/zh_tw