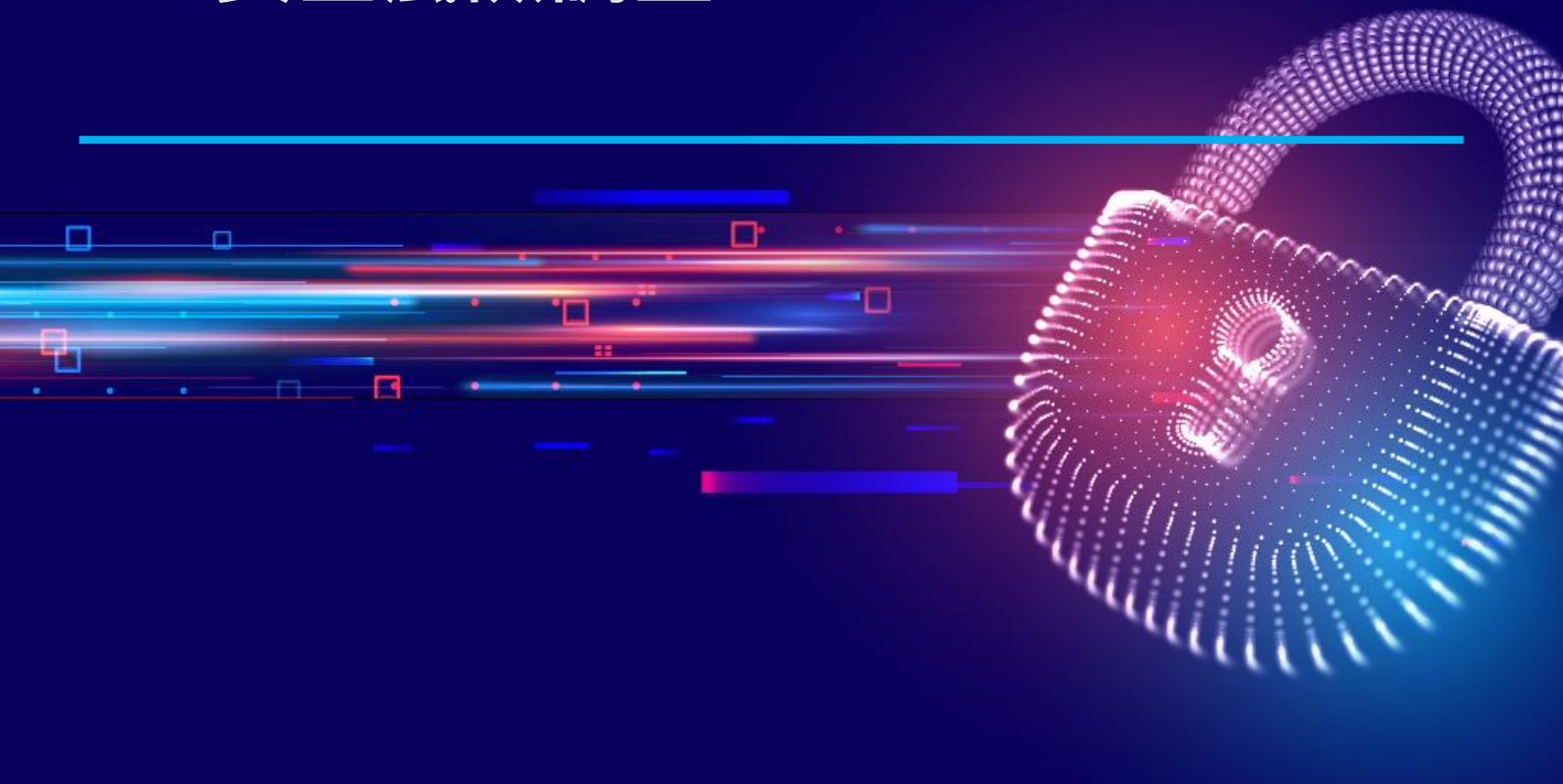
hkpc 生產力局 網絡安全

PCPD HK 香港個人資料私隱專員公署 Office of the Privacy Commissioner for Personal Data, Hong Kong

香港企業網絡保安準備指數及 AI 安全風險調查 2024

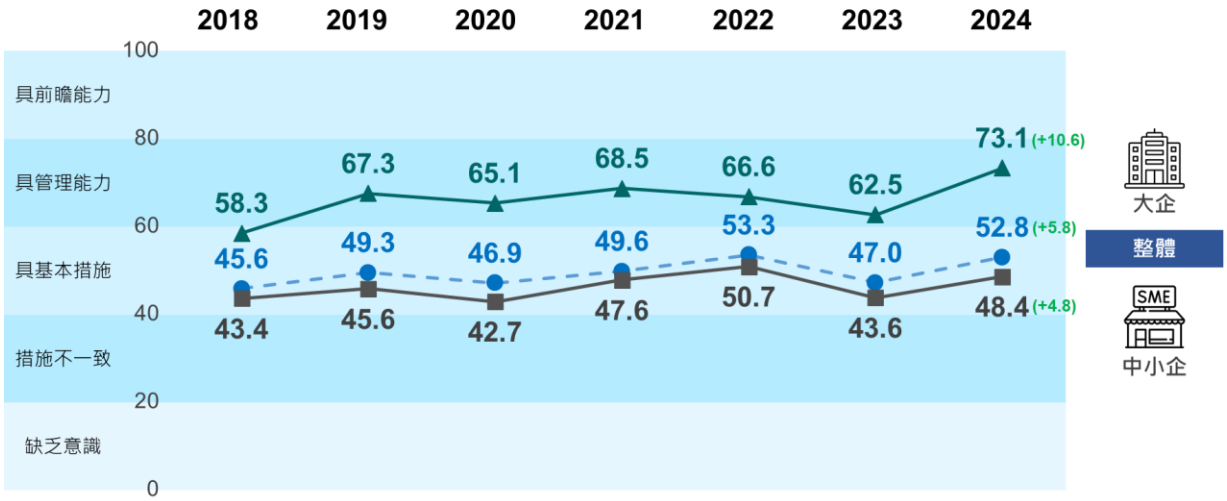


1. 總結及建議

1.1 主要調查結果

香港企業網絡保安準備指數

整體指數上升 5.8 點至 52.8 點，是自 2018 年指數推出以來錄得的最大年度升幅。中小企（48.4 點）和大企[1]（73.1 點）的指數均錄得升幅，當中大企的指數更升至有紀錄以來最高。然而，雖然整體指數有所上升和大企仍然處於「具管理能力」級別，但中小企的網絡安全準備水平仍然維持於「具基本措施」級別。



- *金融服務業*（68.3 點）繼續是指數最高的行業，並保持在「具管理能力」的網絡安全準備水平。
- *資訊和通訊技術業*（58.9 點）是今年唯一一個指數錄得跌幅的行業（-4.4 點），其網絡安全準備水平由「具管理能力」降至「具基本措施」。
- *非牟利機構*、*學校和其他行業*（56.4 點）、*製造*、*貿易和物流業*（50.7 點）以及*專業服務業*（46.0 點）繼續停留在「具基本措施」的網絡安全準備水平。
- *零售和旅遊業*（45.3 點）仍然是所有行業中指數最低的行業。

[1] 大企是指聘用 100 名或以上員工的製造業企業，或聘用 50 名或以上員工的非製造業企業（https://www.success.tid.gov.hk/tc_chi/aboutus/what_are_sme.html）。

企業過去 12 個月遇到的網絡安全攻擊

69%的受訪企業於過去 12 個月內曾遇到最少一類網絡安全攻擊，包括有和沒有導致企業蒙受經濟損失的攻擊。與 2023 年相比，網絡安全攻擊的發生率下跌了 4 個百分點。

「釣魚攻擊」繼續是最普遍的網絡安全攻擊類型，98%於過去 12 個月內曾遇過網絡安全攻擊的企業都表示曾受到此類攻擊。當中，「網絡釣魚電子郵件」（79%）仍然是最常見的釣魚攻擊模式，而「網絡釣魚簡訊」（38%，+4 個百分點）亦較以往常見。另外，7%及 6%於過去 12 個月內曾遇到網絡安全攻擊的企業分別表示曾受到「使用二維碼的釣魚攻擊」及「使用人工智能（AI）或生成式 AI 的釣魚攻擊」等新興的釣魚攻擊。

需持續加強網絡安全風險評估

為了在新興的網絡安全威脅出現前做好準備，並加強對網絡安全攻擊的防禦，全面的政策檢討及系統安全評估對企業來說也是至關重要。

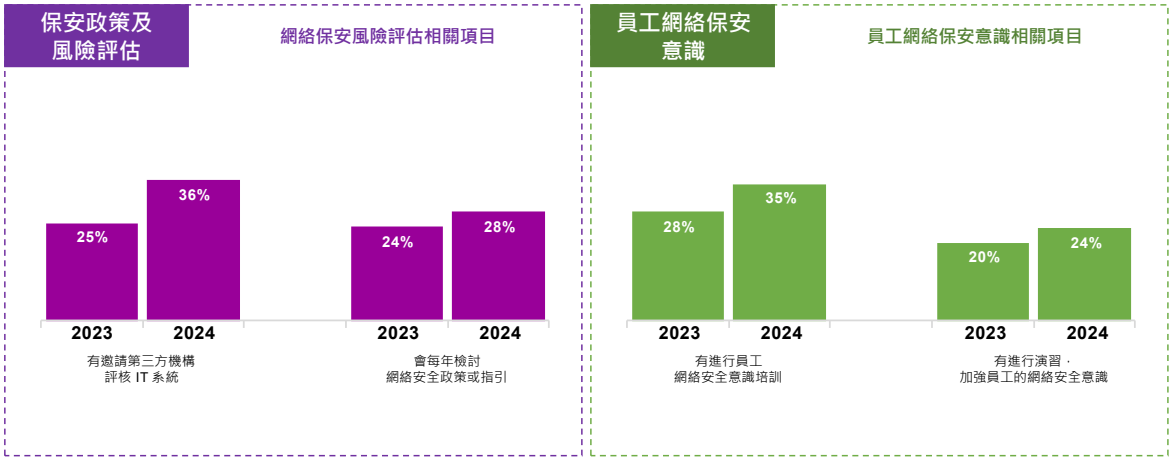
儘管「保安政策及風險評估」分項指數今年有所改善（由 2023 年的 39.7 點升至 2024 年的 52.1 點），但多年來一直維持在「具基本措施」級別（2018 年為 49.4 點，2024 年為 52.1 點）。在過去 12 個月內，只有 36%的受訪企業有聘請第三方機構來評核其 IT 系統，並只有 28%的企業會每年檢討其網絡安全政策。

需提高人員對網絡安全的意識

雖然釣魚攻擊仍然是一個相當棘手的問題，其攻擊類型亦變得多樣化，但是企業可以透過恰當的人員意識教育去預防釣魚攻擊。

在是次調查中，雖然「員工網絡保安意識」有所改善，但該分項指數仍然停留在 30.9 點的低位，處於「措施不一致」級別。令人擔憂的是，只有 35%的受訪企業曾在過去 12 個月內進行員工網絡安全意識培訓，而只有 24%的受訪企業曾進行網絡安全演習。

分項指數 - 有待改善項目



企業對人工智能（AI）技術帶來的私隱風險的認知及運用 AI 技術的情況

調查結果顯示，大多數企業（69%）認為在營運中使用 AI 會帶來顯著的私隱風險。

在使用 AI 方面，約五分之一（21%）的受訪企業現時於營運中使用 AI 技術，而大企（43%）的使用率則較中小企（16%）為高。

在營運中有使用 AI 的企業中，四分之三（75%）的受訪企業表示不會向第三方提供數據。在會向第三方提供數據的企業中，大部分提供公開的數據及匿名化和聚合數據。一般而言，這些數據帶來的私隱風險往往較低。只有少數企業會提供較敏感的數據，例如內部營運數據、個人資料、客戶數據及商業機密（佔 0%至 7%），顯示企業在處理數據及其後續數據傳輸持謹慎態度。

實施數據安全防護措施

於營運中有使用 AI 的企業中，接近三分之二（65%）已經採用了至少一項數據安全防護措施。採取至少一項數據安全防護措施的大企（79%）比例高於中小企（57%）。

企業最常採用的數據安全防護措施包括「存取控制」（41%）及「數據保護措施」（例如加密數據、將個人資料匿名化）（39%）。部分企業亦有採用其他數據安全防護措施，例如「滲透測試」（22%）及「紅隊測試」（15%）。不過，較少企業會使用專門針對機器學習攻擊的保護措施（14%）或設立與 AI 相關的安全警報（13%）。

就使用 AI 而提供 AI 培訓、AI 安全風險政策及個人資料外洩事故應變計劃的情況

在營運中有使用 AI 的企業中，39%有為員工提供有關 AI 的培訓、28%已經制訂 AI 安全風險政策，以及 16%已制訂應對 AI 相關的資料外洩事故應變計劃。

調查亦發現，中小企就使用 AI 而提供培訓、制訂 AI 安全風險政策及個人資料外洩事故應變計劃的情況較不普遍：

1. 約一半（52%）的中小企已經提供或計劃會為員工提供 AI 的培訓，而大企的數字為 82%；
2. 較少中小企已經制訂或計劃制訂 AI 安全風險政策（中小企有 45%，大企則有 74%）；
3. 只有 10%在營運中使用 AI 的中小企有制訂涵蓋應對 AI 相關的個人資料外洩事故應變計劃，而大企則有 26%。

使用 AI 技術加強數據安全及網絡安全的計劃

接近一半的受訪企業（47%）計劃在未來 12 個月內加強網絡安全，當中約一半的企業希望增加使用 AI 技術以加強網絡安全和數據安全（22%），相當於所有受訪企業的約五分之一。

87%的受訪大企計劃在來年加強網絡安全，當中接近一半的受訪大企（46%）希望透過增加使用 AI 技術以實現此目的及加強數據安全。相比之下，較少中小企計劃加強網絡安全，只有 38%的中小企有此計劃，但值得留意的是，計劃使用 AI 以加強網絡和數據安全的中小企的比例（17%，即 38%的約一半）與大企相似。

1.2 建議

因應調查結果，報告對企業有下列建議：

(1) 大企應繼續保障網絡安全；面對較高風險的中小企應將網絡準備水平提升至「具管理能力」級別

大企的整體企業網絡保安準備指數顯著上升，今年指數更升至有紀錄以來最高。雖然有此進展，但鑑於大企擁有較多員工及較大的業務規模，大企應繼續將保障網絡安全視為重要任務，並致力維持在「具管理能力」級別或甚至提升至更高級別。

另一方面，中小企的指數多年來只有微小的升幅，並仍停留在「具基本措施」級別。中小企應考慮其風險承擔程度，以決定應否進一步加強網絡安全準備，並致力達到更高的水平。在評估風險承擔程度時，企業應考慮各種因素，例如企業所持有或處理的數據的數量和敏感程度、業

務是否牽涉對外的網上服務（例如經營網上商店），以及發生網絡安全攻擊對企業的營運及聲譽帶來的潛在影響。

企業應考慮強化較弱的範疇，尤其是「員工網絡保安意識」。該指數仍然停留在 30.9 點的低水平。「保安政策及風險評估」是另一個需改善的重要範疇，因為自指數成立以來，這範疇的改進幅度較小。

為加強網絡安全，建議機構採取以下網絡安全措施：

- **全面性及定期的更新**
  - 擴大風險評估範圍：確保風險評估涵蓋機構的每個範疇，包括物聯網設備、自攜設備（BYOD）、雲端服務及第三方供應商。這有助於識別潛在漏洞，並評估供應鏈風險。
  - 定期評核及更新：持續評核和更新風險評估及政策，以應對機構技術環境的變化、新興威脅及監管要求。
- **採用及適應網絡安全框架**
  - 採用具聲譽的框架：採用行之有效的網絡安全框架，例如 NIST 或 ISO/IEC 27001。這些框架能提供系統性的指引，以管理和改進安全狀況。
  - 定制框架：根據機構的具體需求和背景定制所選框架，確保其與業務目標和監管責任保持一致。
- **實施反饋循環**
  - 評核事故及從中學習：在安全事故發生後，進行全面評核，以識別事故原因，並相應地更新政策和程序。

(2) 透過教育提高網絡安全意識

人員一直是網絡安全中最致命的弱點。然而，網絡安全意識教育通常是在經歷網絡安全攻擊後，才被視為首要任務。在是次調查中，「釣魚攻擊」仍然是企業最常面對的網絡安全攻擊類型，幾乎所有在過去 12 個月內遇到攻擊的企業都受到此類攻擊。事實上，「釣魚攻擊」利用人員的弱點作攻擊，例如一名員工意外打開一個有勒索軟件的附件，或點擊進入釣魚連結時，就有機會導致企業伺服器上的數據被加密，並不能再度存取。

因此，建議企業透過以下方式提高人員的網絡安全意識：

- 定期為所有一般員工及新入職員工提供培訓，並鼓勵他們在網絡安全員工培訓平台（https://cyberhub.hk/）接受針對人員進行角色為基礎的培訓；
- 參加 HKCERT 及個人資料私隱專員公署（私隱專員公署）舉辦的網絡安全研討會，了解新興的網絡威脅和新技術的風險；

- 定期進行釣魚測試及網絡安全演習，監測表現並處理表現較弱的範疇；
- 高級管理層公開推廣網絡安全文化；
- 瀏覽 HKCERT 的「網絡釣魚 全城防禦」主題網站，該網站是一個「一站式」且易於使用的防釣魚資訊網站，而且提供企業使用的現成材料，以對員工進行釣魚意識培訓（https://www.hkcert.org/tc/publications/all-out-anti-phishing）；
- 瀏覽私隱專員公署的「數據安全」主題網站，該網站提供「一站式」有關數據安全的資訊，並協助資料使用者遵從《個人資料（私隱）條例》的規定（https://www.pcpd.org.hk/tc_chi/data_security/index.html）；
- （適用於中小企）下載《中小企保安事故應變指南》（https://www.hkcert.org/tc/security-guideline/incident-response-guideline-for-smes），了解預防和處理網絡安全攻擊的行動和程序；及
- 參考私隱專員公署發布的指引，包括《資料外洩事故的處理及通報指引》（https://www.pcpd.org.hk/tc_chi/resources_centre/publications/files/guidance_note_dbn_c.pdf）及《資訊及通訊科技的保安措施指引》（https://www.pcpd.org.hk/tc_chi/resources_centre/publications/files/guidance_datasecurity_c.pdf）。

為協助學校、非牟利機構及中小企加強保障數據安全、網絡安全，私隱專員公署已在 2024 年 10 月推出「數據安全」套餐，參加的機構可免費進行「數據安全快測」，評估其數據安全措施是否足夠，並在完成「快測」後享有免費名額參加由公署舉辦的研習班及講座。

(3) 改善政策評核及系統安全評估

為了應對新興威脅，企業應主動採取措施，定期評核其安全政策和指引，並進行全面的系統安全評估。建議企業採取以下措施：

- **年度政策審查**：企業應至少每年評核一次內部政策及指引，以確保機構對釣魚、勒索軟件及其他類型的網絡安全攻擊等不斷演變的威脅保持警惕和有所準備。通過追蹤最新的網絡安全趨勢和最佳行事方式，企業可以識別現有政策中的漏洞，並作出必要的調整以應對新的弱點。

- **利用第三方系統安全風險評估服務**：由於獨立的安全風險評估可以提供對機構安全狀況的客觀評估，並幫助識別內部團隊可能忽略的漏洞，企業應考慮聘用第三方系統安全風險評估服務。重要的是，企業應優先對牽涉對外的網上系統或服務進行評估，因為這些系統或服務更容易面臨外部威脅，並且通常是網絡安全攻擊的主要目標。

(4) 安全、負責任及以私隱友善的方式使用 AI 技術

隨著 AI 的使用量增加，企業必須確保安全和負責任地應用 AI，以應對和減輕其固有風險，包括個人資料私隱風險。目前，儘管 65%有使用 AI 技術的企業已經採用了數據安全防護措施，但少於一半的企業制訂了 AI 安全風險政策、為員工提供 AI 相關的培訓，以及制訂應對 AI 相關的資料外洩事故應變計劃。因此，強烈建議企業採取適當的行動來彌補不足之處，並防止因使用 AI 技術帶來的私隱風險。

為了以安全、負責任及以私隱友善的方式的方式使用 AI 技術，建議企業通過以下方式加強 AI 安全：

- **利用 AI 技術檢測及識別網絡安全威脅，並實施自動化應對措施**
    - 檢測：AI 可以持續監控系統和網絡，識別潛在安全威脅的異常模式或行為，例如未經授權的存取、異常數據傳輸或不正常的登入時間。AI 演算法還可以實時分析大量數據，即時偵測潛在威脅的出現；
    - 識別：AI 可以根據威脅的嚴重性和潛在影響對其進行分類，協助網絡安全團隊根據威脅的嚴重性和影響決定處理的優先次序。通過在早期階段識別威脅的性質和嚴重性，企業可以更有效地分配資源以防微杜漸；及
    - 自動化應對：AI 可以自動對檢測到的威脅作出初步應對，例如隔離受影響系統、封鎖惡意 IP 地址，及/或終止可疑程序等，以快速遏制威脅，減少潛在損害並將營運受阻程度降至最低。
- **實施足夠的措施以保護 AI 系統的數據安全**：採用數據安全防護措施，例如設置存取控制、進行紅隊測試、採用數據保護措施（例如數據加密及個人資料匿名化）、採取對抗機器學習攻擊的保護措施、進行滲透測試，以及設立與 AI 相關的安全警報。採用足夠的措施可以幫助保護 AI 系統免受網絡安全攻擊，確保數據（包括個人資料）的安全，並減低數據外洩的風險。
- **制訂全面的政策以加強 AI 安全**：採納國際公認的最佳行事方式，以在制訂 AI 安全政策時，確保整個 AI 生命周期內的數據安全。舉例而言，企業可以考慮採用由國際標準化組織等專業協會制訂和發布的國際標準和指南。
- **制訂 AI 事故應變計劃**：參考私隱專員公署在《人工智能（AI）：個人資料保障模範框架》(《模範框架》) 中的建議，建立全面的計劃。《模範框架》建議制訂 AI 事故相關的應變計劃，以監控和處理可能意外發生的事故。該計劃可以涵蓋界定、監察、通報、遏止、調查 AI 事故及從 AI 事故中復原之要素。企業亦應制訂一個能應對為 AI 相關事故而設的資料外洩事故應變計劃，以應對 AI 事故中可能出現的資料外洩事故。
- **為員工提供足夠的 AI 培訓**：為員工提供足夠的培訓，以確保他們具備適當的知識、技

能及認知，協助企業恰當地實施有關 AI 的政策，並培養負責任使用 AI 的文化。鑒於企業在營運上的多樣性，採用通用的培訓方法未必理想。因此，建議培訓應因應員工的崗位進行，即視乎企業營運的性質，針對不同崗位的特定需求和職責提供定制的培訓內容，以確保每位員工能就其在崗位上如何使用 AI 接受最相關和合適的培訓。