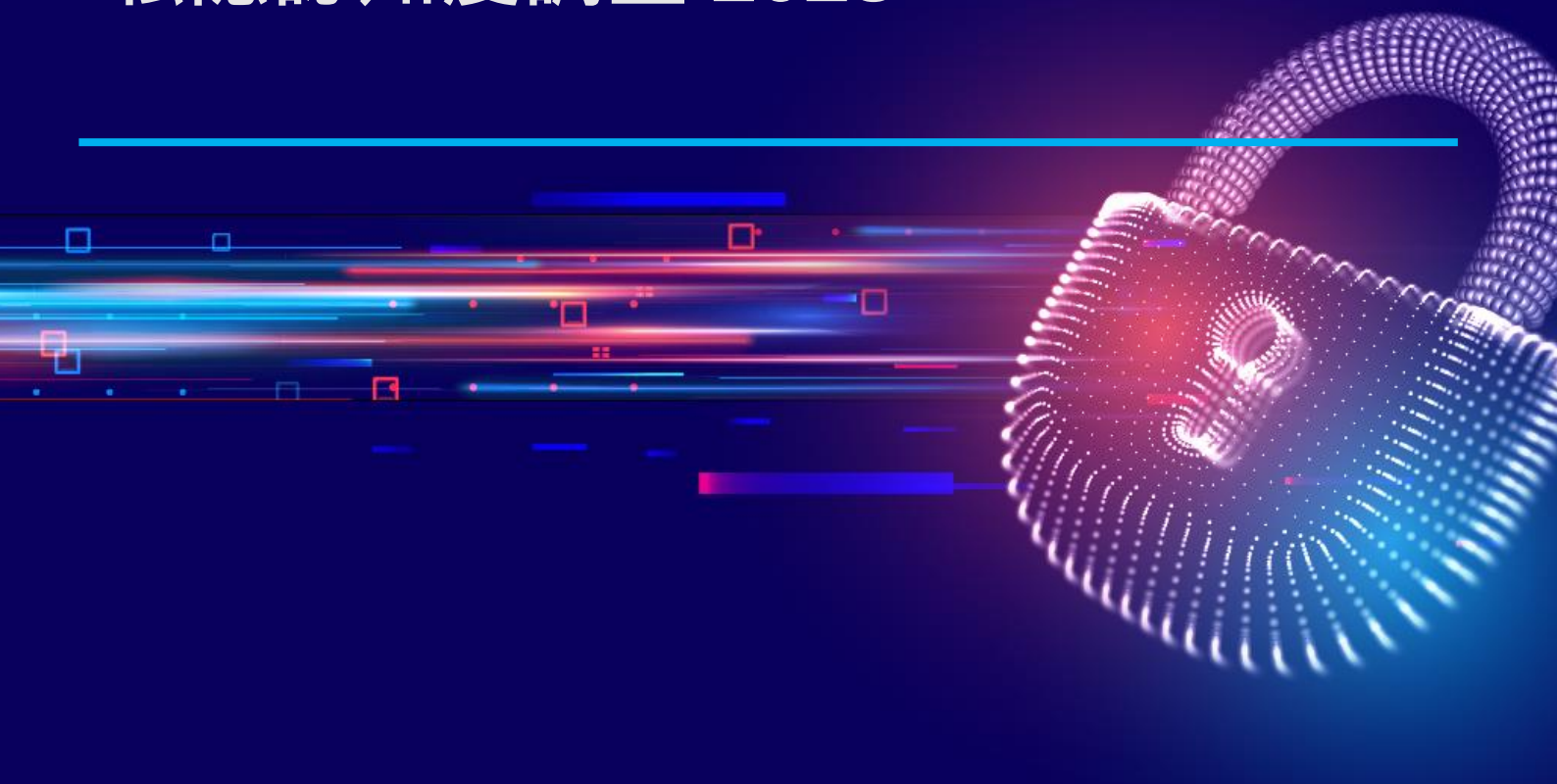
hkpc 生產力局 網絡安全

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私隱認知度調查 2023

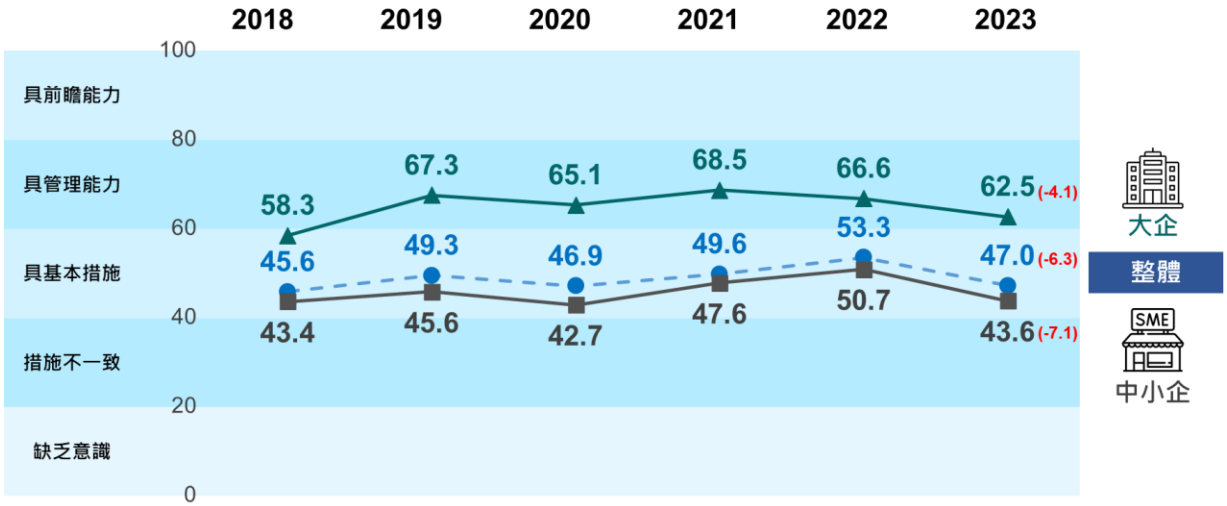


1. 總結及建議

1.1 主要調查結果

香港企業網絡保安準備指數

整體指數下跌 6.3 點至 47.0 點，是自 2018 年指數推出以來錄得的最大跌幅。中小企（43.6 點）和大企[1]（62.5 點）的指數都有所下跌，當中中小企的指數的跌幅較大（-7.1 點）。儘管大企的指數再度下跌 4.1 點，但仍維持在「具管理能力」的水平。



金融服務業（64.9 點）及*資訊和通訊技術業*（63.3 點）仍然保持在「具管理能力」的網絡安全準備水平，而後者更是唯一一個指數錄得升幅的行業。雖然*製造*、*貿易和物流業*（48.6 點）、*非牟利機構*、*學校和其他行業*（45.9 點）及*專業服務業*（43.5 點）均錄得不同程度的跌幅，但仍然維持在「具基本措施」水平。然而，*零售和旅遊業*（33.3 點）錄得的跌幅最大，下跌 12.5 點至「措施不一致」網絡安全準備水平。

企業過去 12 個月遇到的網絡安全攻擊

73%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，不論這些攻擊是否導致企業承受經濟損失。與 2022 年相比，網絡安全攻擊的發生率顯著上升 8 個百分點至歷來新高，而其於中小企的發生率更大幅上升達 10 個百分點。

「釣魚攻擊」繼續是最普遍的網絡安全攻擊類型，96%於過去 12 個月內曾遇到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%）繼續是最常見的釣魚攻

[1] 大企是指聘用 100 名員工或以上的製造業企業，或聘用 50 名員工或以上的非製造業企業。

擊模式，而「網絡釣魚簡訊」（34%，+14 百分點）及「社交媒體釣魚」（16%，+6 百分點）亦較以往常見。另外，9%及 8%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「使用人工智能（AI）或生成式 AI 的釣魚攻擊」及「使用二維碼的釣魚攻擊」等新興的釣魚攻擊。

受訪企業遇到的網絡安全攻擊類型（外部攻擊，內部攻擊及對外合作夥伴引起的攻擊）方面，外部攻擊繼續飆升 13 個百分點至歷來新高 72%。雖然內部攻擊的發生率跌至 3%的低水平，但由外部合作夥伴引起的攻擊的發生率，即使較去年改善至 7%，數字仍然相對較高。

需提高人員對網絡安全的意識

即使網絡安全水平較過去有所提高，而且大多數網絡安全攻擊可以被偵測及預防，但人員仍然是網絡安全的關鍵。「人員意識」能協助預防網絡安全攻擊發生。然而，是次調查結果反映這方面的意識並沒有明顯改善：

1. 「人員意識」分項指數仍然停留在 25.2 點的低位，處於「措施不一致」水平的邊緣；
2. 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，但是這些攻擊可以透過恰當的人員意識教育去預防。然而，在是次調查中，仍然只有 28%的受訪企業曾在過去 12 個月進行員工安全意識培訓，另外更只有五分之一的企業曾進行網絡安全演習。

實施個人資料私隱管理系統（PMP）和實踐保護私隱及資料保安的措施

調查發現，大企實施 PMP 和實踐各種保護私隱及資料保安的措施的情況較普遍：

1. 近一半（48%）的大企已「完全實施」PMP，但 55%的中小企「未有計劃實施」；及
2. 79%的大企已經實踐至少一項保護私隱及資料保安的措施，但中小企的相關數字只得 54%。

企業所採取的保護私隱及資料保安的措施方面，其中一些較常實踐的措施屬 PMP 組件內*機構的決心*及*系統管控措施*，包括：

1. 75%已制訂處理個人資料的內部政策；
2. 63%在過去 24 個月內於董事會會議和 / 或高級管理層會議上討論和肯定 PMP 的重要性；
3. 55%有個人資料外洩通報機制；及
4. 53%向員工提供有關私隱的培訓，包括有關《個人資料（私隱）條例》的培訓。

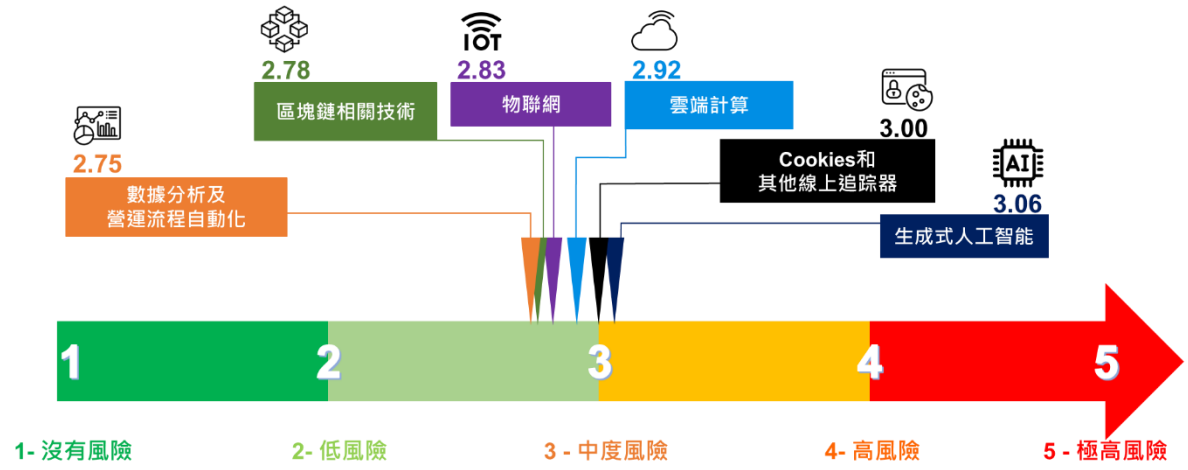
另一方面，實踐 PMP 內*持續評估及修訂*組件相關的措施（例如有關個人資料處理方式 / 個人資料私隱管理系統的持續審查程序）則比較少見（46%）。其他較少企業實踐的 PMP 措施包括：

1. 有個人資料外洩應變計劃（46%）；
2. 有保障資料主任，或專門的保護個人資料的部門（44%）；及
3. 有政策就涉及個人資料的項目 / 計劃進行私隱影響評估（41%）/ 曾進行過私隱影響評估（39%）。

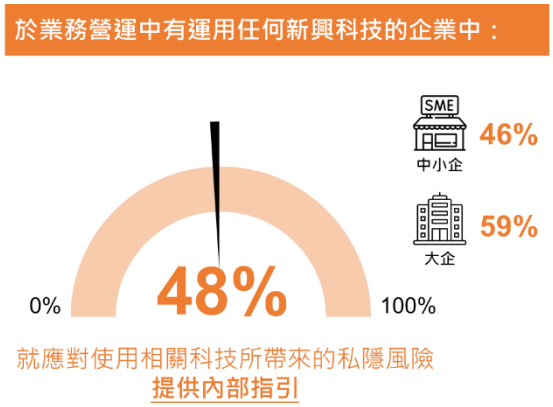
運用新興科技和對新興科技所帶來的私隱風險的認知

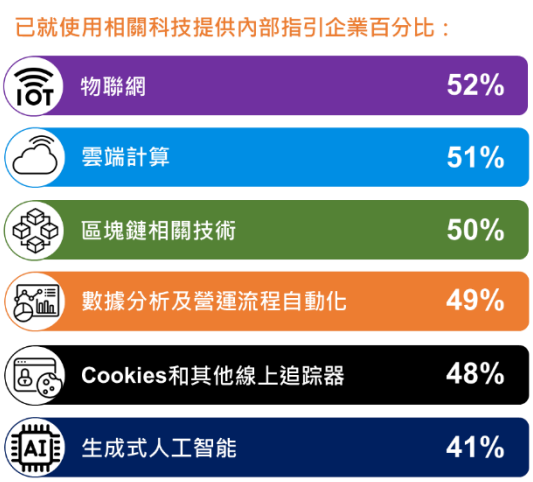
企業不論是否運用新興科技，即生成式人工智能、數據分析及營運流程自動化、物聯網（IoT）、區塊鏈相關技術、雲端計算及 Cookies 和其他線上追踪器科技，都有留意到運用這些科技所涉及的私隱風險，平均值由 2.75 至 3.06（即介乎「低風險」和「中風險」之間）。

當中，企業認為「生成式人工智能」（3.06）和「Cookies 和其他線上追踪器」（3.00）所涉及的私隱風險最高，其次是「雲端計算」（2.92）、「物聯網」（2.83）及「區塊鏈相關技術」（2.78）。



儘管運用不同新興科技的企業都注意到運用相關科技可能涉及私隱風險，但整體只有接近一半（48%）企業就應對使用相關科技所帶來的私隱風險提供內部指引，而就使用生成式人工智能提供相關指引的企業更低，只有 41%。





企業對香港的個人資料私隱保障水平的整體看法

大部分受訪企業中對於能夠遵守《個人資料（私隱）條例》表示有信心，當中 42%認為「沒有困難」，而 34%認為「有一些困難」。

就香港的個人資料私隱保障水平方面，稍高於一半（51%）的受訪企業持中立態度，而 18%則認為私隱保障「充足」或「非常充足」。

「數據處理漸趨複雜」（39%），「缺乏員工知識或教育」（37%）及「資源不足」（36%）是企業認為遵守《個人資料（私隱）條例》的三大主要挑戰。

1.2 建議

因應調查結果，報告對企業有下列建議：

(1) 將網絡安全準備水平提升至「具管理能力」級別，並適時採取網絡安全及資料保安措施

儘管網絡威脅不斷升級，越來越多的企業繼續將其業務數碼化。尤其是在疫情影響下，越來越多活動數碼化，預料這趨勢將會持續。多年來，總體企業網絡安全準備指數一直停留在「具基本措施」水平，而今年更錄得歷來最大跌幅。企業，特別是規模較小的企業，應進一步加強網絡安全準備水平，並提升至「具管理能力」級別。

要得到最大改善，企業可先從較弱的範疇著手，特別是「人員意識」方面。該指數仍然停留在 25.2 點的低水平。「政策和風險評估」是第二個需急切改善的範疇。是次調查發現，由於企業在執行「安全風險評估」措施方面有所鬆懈，指數下跌 8.9 點至「措施不一致」級別。如果資源許可，企業亦可以檢討和加強「技術控制」下，關於「系統保安修補管理」和「網絡威脅防禦措施」的措施。

為加強網絡與數據安全，防範資訊系統受到惡意攻擊，所有機構亦應防患未然，增強對網絡安全的意識，審視數據保安系統，並適時採取以下網絡安全及資料保安措施：

- 保護電腦網絡：使用保安裝置或軟件（例如防火牆及／或反惡意軟件應用程式）以保護電腦網絡，並定期更新軟件（包括電話應用程式及反惡意軟件應用程式）以偵測新病毒及威脅；
- 定期對資訊及通訊系統進行保安漏洞評估及滲透測試，尤其與互聯網連接的系統；
- 實施修補程式的管理，以適時修補保安漏洞；
- 加密傳輸中和存儲中的資料，有效地管理和保護加密密鑰；
- 管理資料庫：利用防火牆將資料伺服器與網絡伺服器分開；
- 採用「最小權限」的原則，授予用戶盡可能少的存取權限以完成工作，並將適當的角色分配給用戶（包括限制存取資料的數量和時間）；及
- 適時地銷毀不必要的或過期的個人資料。

為加強資料保安系統，私隱專員公署已於 2022 年 8 月刊發《資訊及通訊科技的保安措施指引》，為持有個人資料的機構提供一些切實可行的建議資料保安措施。

(2) 透過教育提高網絡安全意識

人員一直是網絡安全最薄弱一環。然而，網絡安全意識教育通常是在經歷網絡攻擊後，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，或點擊進入釣魚鏈結時，就有機會導致企業伺服器上的數據被加密，並不能再度連接。

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/）接受培訓，或參加私隱專員公署的培訓；
- 定期進行網絡安全演習，監測表現並處理較弱的範疇；

- 參加有關網絡安全的研討會，訂閱安全諮詢以獲取有關網絡安全攻擊和解決方案的最新信息；
- 加入網絡安全資訊共享夥伴計劃（https://www.cybersechub.hk/en/home/highlights）或私隱專員公署的保障資料主任聯會（https://www.pcpd.org.hk/misc/dpoc/index.html），交流信息並與業內同行建立共同防禦網；
- 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/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）；
- 訂閱能提供全面網絡保安方案的網絡保安託管服務（MSS）。它能主動和快速偵測網絡安全攻擊並迅速作出反應之餘，同時了解攻擊的規模和性質、內部控制和殘留風險；及
- （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。

(3) 網絡保安託管服務

網絡安全管理的四大挑戰仍然與人才和投資相關，包括「欠缺 IT 支援及管理人手」（44%）、「網絡保安需求隨時間變化，需要多樣化的投資」（42%）、「需要龐大的基建投資」（38%）和「欠缺相關專才或技術」（37%）。同時，大多數受訪企業在網絡安全方面的支出都在 99,999 港元或以下。

企業可以考慮訂閱網絡保安託管服務，它以將網絡安全專業外判的方式，應對上述網絡安全管理的挑戰。其設置成本較低，並提供靈活的價格選擇，同時亦能獲得網絡安全專家的全面支援。

(4) 建立 PMP 及採取資料保護措施

調查發現，相比大企，較少中小企實踐個人資料保護措施和實施 PMP。報告建議所有企業應建立妥善的 PMP，以幫助企業循規地收集、持有、處理和使用個人資料，加強數據管理及確

保數據安全。私隱專員公署已發布《私隱管理系統 — 最佳行事方式指引》，為企業建立全面私隱管理系統方面提供框架，並輔以具體例子及實用建議以供參考，當中包括採取以下措施：

- 於董事會會議和 / 或高級管理層會議上討論個人資料私隱的議題；
- 制訂處理個人資料的內部政策；
- 對涉及個人資料的項目進行私隱影響評估；
- 設立保障資料主任或專門的保護個人資料的部門；
- 向員工提供私隱培訓，包括《個人資料（私隱）條例》的培訓；以及
- 制定有關於個人資料處理方式 / 個人資料私隱管理系統的持續審查程序。

為了進一步保護個人資料安全和網絡安全，企業亦應制定個人資料外洩應變計劃和個人資料外洩通報機制，以防範網絡攻擊和 / 或個人資料外洩事件。企業可參考私隱專員公署於 2023 年 6 月發出的《資料外洩事故的處理及通報指引》做好準備，一旦發生資料外洩事故可以有效地應對。企業亦可參加由私隱專員公署舉辦的私隱管理系統專業研習班，了解私隱管理系統的基本原則及必要組件，以及如何持續維持及改善私隱管理系統。

(5) 有責任地使用新興科技

雖然企業，尤其是大企，使用一般被認為發展較成熟的新興科技（例如雲端計算、數據分析及營運流程自動化，以及 Cookies 和其他線上追踪器）的情況較普遍，但企業對這些科技所意識到的私隱風險水平相比其他新興科技並無明顯分別，大致上屬「中風險」水平，可見科技的成熟程度並不一定與所意識到的私隱風險水平有關。報告鼓勵所有企業在使用新興科技時保持警惕，留意潛在的私隱風險。

隨著新興科技的使用預料增加，企業必須確保正確使用有關科技，以應對相關私隱問題。鑒於有使用新興科技的受訪企業提供內部指引以應對相關私隱風險並不普遍，報告呼籲企業訂立適當的內部指引，以應對使用新興科技所涉及的私隱風險。