

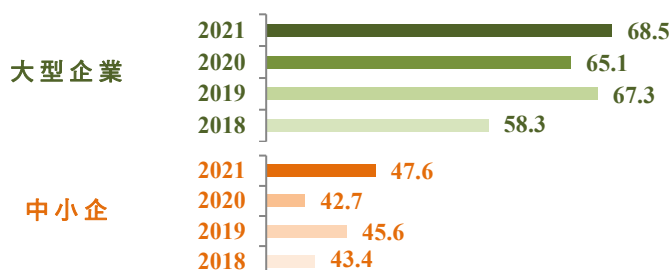
香港中小企的網絡安全挑戰

圖1 — 按企業規模劃分的使用互聯網和採用電子商貿情況^(a)

	2017		2019		2021	
	大型企業 (%)	中小企 (%)	大型企業 (%)	中小企 (%)	大型企業 (%)	中小企 (%)
使用互聯網	99.8	87.4	99.5	90.1	100.0	95.6
擁有本身的網站/網頁	88.2	32.5	88.1	37.3	91.6	42.9
在網上獲取訂單	19.1	7.3	24.1	8.7	26.1	11.0
在網上採購	34.1	21.0	35.2	20.9	37.3	24.7

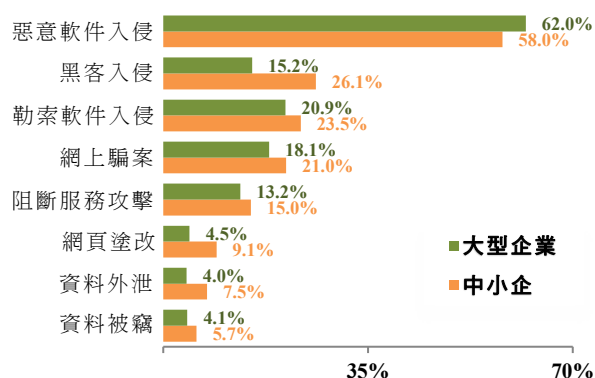
註：(a) 企業規模按其就業人數分類為大型企業及中小企。大型企業指(i)聘用多於100名員工的製造業單位；或(ii)聘用多於50名員工的非製造業單位。其他規模的企業則定義為中小企。

圖2 — 2018年至2021年間的網絡保安準備指數^(a)



註：(a) 指數按0至100評分，就以下4個範疇評核企業的網絡保安措施是否全面：(i)保安政策風險評估；(ii)技術控制；(iii)流程控制；及(iv)建立員工意識。

圖3 — 曾遭遇網絡保安事故的企業比例^{(a)·(b)}



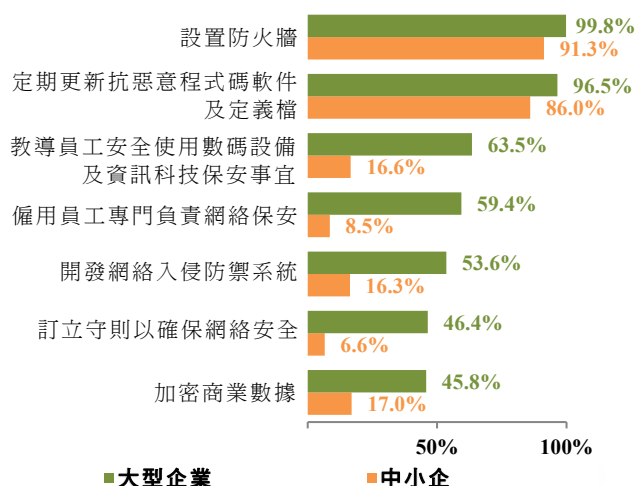
註：(a) 統計期間，1 024間大型企業及26 929間中小企曾遭遇網絡保安事故。同一家企業可以遭遇多於一種事故。
(b) 圖中百分比指曾遭遇某一種網絡保安事故的企業，在所有相應規模且曾遭遇網絡保安事故的企業中所佔的比例。

重點

- 香港的企業絕大部份為中小型企業（“中小企”），它們的蓬勃發展與商業表現對本港經濟尤為重要。近年，使用數碼途徑協助營商，並且擁有本身的網站/網頁的中小企比例與日俱增(圖1)，無形中收窄了與大型企業之間的數碼鴻溝。自2020年年初爆發2019冠狀病毒病疫情後，這勢頭更見明顯，越來越多中小企透過電子商貿途徑獲取訂單及/或進行購買活動。
- 然而，中小企應對網絡安全威脅的準備工作，仍較大型企業不足。根據香港生產力促進局（“生產力促進局”）自2018年起每年進行的調查，中小企的網絡保安準備指數一直低於50(圖2)，而它們與大型企業指數之間的差距，亦較2018年的幅度為大，這或與大型企業在相關期間加強其網絡防禦能力有關。
- 政府統計處曾於2020年至2021年期間，就工商業使用資訊科技的情況進行另一項統計調查。調查結果顯示，每12間中小企之中，便有約一間曾於統計期內遭遇網絡保安事故。按事故類別分析，“惡意軟件入侵”是中小企最常見的網絡保安事故，其次是“黑客入侵”、“勒索軟件入侵”及“網上騙案”(圖3)。此外，與大型企業相比，中小企普遍較容易受黑客入侵、網頁塗改攻擊及資料外泄等威脅。
- 科技罪案亦是商界日益關注的問題。根據香港警務處的資料，2021年的科技罪案總數按年增加約25%至16 200宗左右。在近期的科技罪案中，騙徒常用的犯案手法是先入侵中小企的電郵系統，假冒受害公司的業務夥伴(如供應商)及/或高層向員工發出電郵，以業務需要為由，要求匯款至騙徒操控的帳戶。2021年，與電郵騙案有關的損失金額超過15億港元，佔整體科技罪案損失總金額的一半，超過七成電郵騙案的受害者為中小企。

香港中小企的網絡安全挑戰(續)

圖4 — 2021年企業採用的選定網絡保安措施(a)·(b)



註：(a) 同一家企業可採用多於一種措施。
(b) 圖中百分比指採用特定網絡保安措施的企業，在所有相應規模且有採用網絡保安措施的企業中所佔的比例。

圖5 — 2021年企業應對網絡保安危機的主要困難

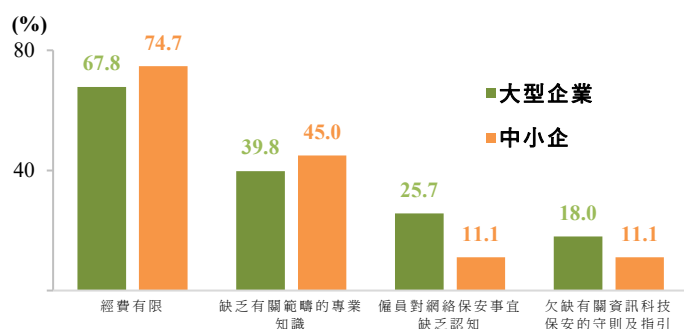
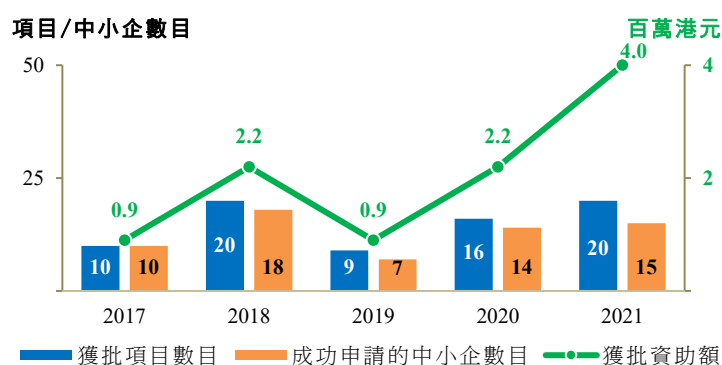


圖6 — 2017年至2021年間獲“科技券”計劃資助的網絡保安解決方案



重點

- 企業投放於特定網絡保安範疇的開支，亦反映它們對數碼領域安全的重視程度。雖然中小企在設置防火牆與定期更新抗惡意程式碼軟件及定義檔方面，大致上可媲美大型企業，惟它們在聘請網絡安全專家、為員工提供資訊科技保安培訓或指引，以至訂立網絡保安守則等涉及員工的範疇卻與大型企業存在較大差距(圖4)。
- 儘管生產力促進局建議商業機構應多着眼於“網絡保安意識培訓”及“網絡威脅偵測”等較弱領域，但中小企與大型企業的體會不同，前者對“提升僱員網絡保安意識”及“制訂資訊科技保安指引”表示困難的比例較後者少(圖5)。這或許是中小企投放於與人力資源相關的保安措施開支較少的原因之一。與此同時，企業無論規模大小，均認為“經費有限”和“缺乏有關範疇的專業知識”是應對網絡保安問題的兩大障礙。
- 本港企業可透過政府或其他機構提供的各種資源，以加強網絡安全，當中包括申領“科技券”計劃的資助。“科技券”計劃於2016年推出，旨在支援非上市本地企業開發各類資訊科技系統，包括提升它們網絡防禦能力的網絡保安項目。根據政府資訊科技總監辦公室(“資科辦”)的資料，“科技券”計劃於2017年至2021年期間共批出75個涉及網絡安全的項目，當中中小企獲批數目達64宗(圖6)。
- 除提供資助外，資科辦亦一直致力支援中小企提升網絡安全意識，並夥拍其他非政府機構推出各種支援措施，包括設立事故報告熱線、舉辦資訊科技安全講座、為中小企網站提供免費掃描服務，以至提供有關網絡安全狀況的線上自我評估工具。例如，資科辦正與香港互聯網註冊管理有限公司合作，於2022年底編製一系列適用於不同行業中小企的培訓教材，以提高僱員的網絡安全意識。

數據來源：創新及科技局、政府統計處、香港警務處、政府資訊科技總監辦公室、香港生產力促進局及香港電腦保安事故協調中心的最新數據。

立法會秘書處
研究及資訊部
資料研究組
2022年6月30日
電話：3919 3181

數據透視為立法會議員及立法會轄下委員會而編製，它們並非法律或其他專業意見，亦不應以該等數據透視作為上述意見。數據透視的版權由立法會行政管理委員會(下稱“行政管理委員會”)所擁有。行政管理委員會准許任何人士複製數據透視作非商業用途，惟有關複製必須準確及不會對立法會構成負面影響。詳情請參閱刊載於立法會網站(www.legco.gov.hk)的責任聲明及版權告示。本期數據透視的文件編號為 ISSH18/2022。