
hkirc
香港互聯網註冊管理有限公司

物聯網與網絡保安

調查結果公佈

2019

議程

- 目的
- 物聯網的定義
- 調查方法
- 「物聯網與網絡保安」調查結果
  - 1. 使用物聯網的情況
  - 2. 使用物聯網的保安意識
  - 3. 公眾對物聯網安全教育的看法
- 總結

01 物聯網概述

調查目的

- 了解公眾對物聯網與資訊保安的：
  - 使用情況及模式
  - 用戶意識
  - 降低網絡安全風險行為
  - 安全教育的看法

物聯網的定義

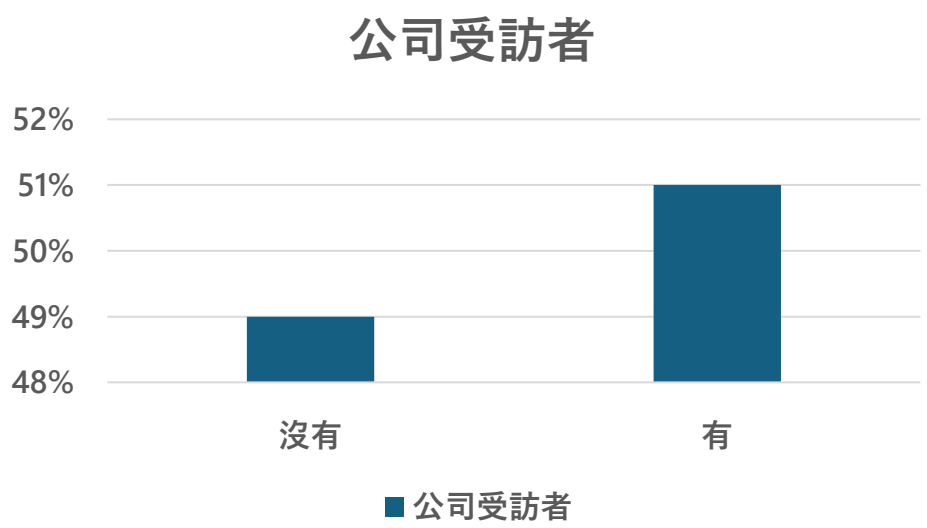
- 在本報告中， 物聯網泛指由實體裝置， 如Wi-Fi路由器、隨身智能手環、智能照明系統、智能門鎖及家用電器等等， 經由感應器(sensor)和應用程式介面 (API) 等裝置， 透過網際網路所形成的訊息連結與交換網路

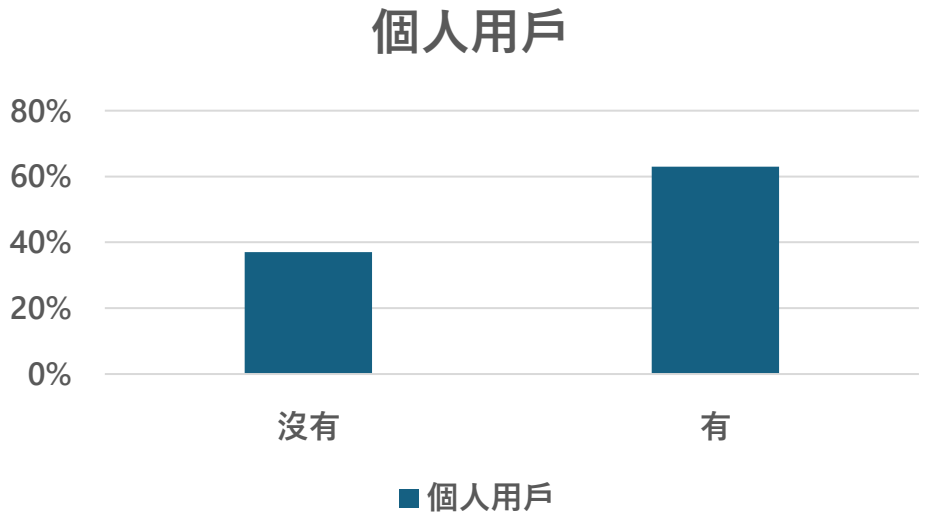
調查方法

- 調查期限 ：
  - 2019年7月26日至8月6日
- 參與調查人數 ：
  - 713人
- 完整及有效的回覆：
  - 564個
- 推廣方法：
  - 電子郵件、網上及社交媒體

02 使用物聯網的情況

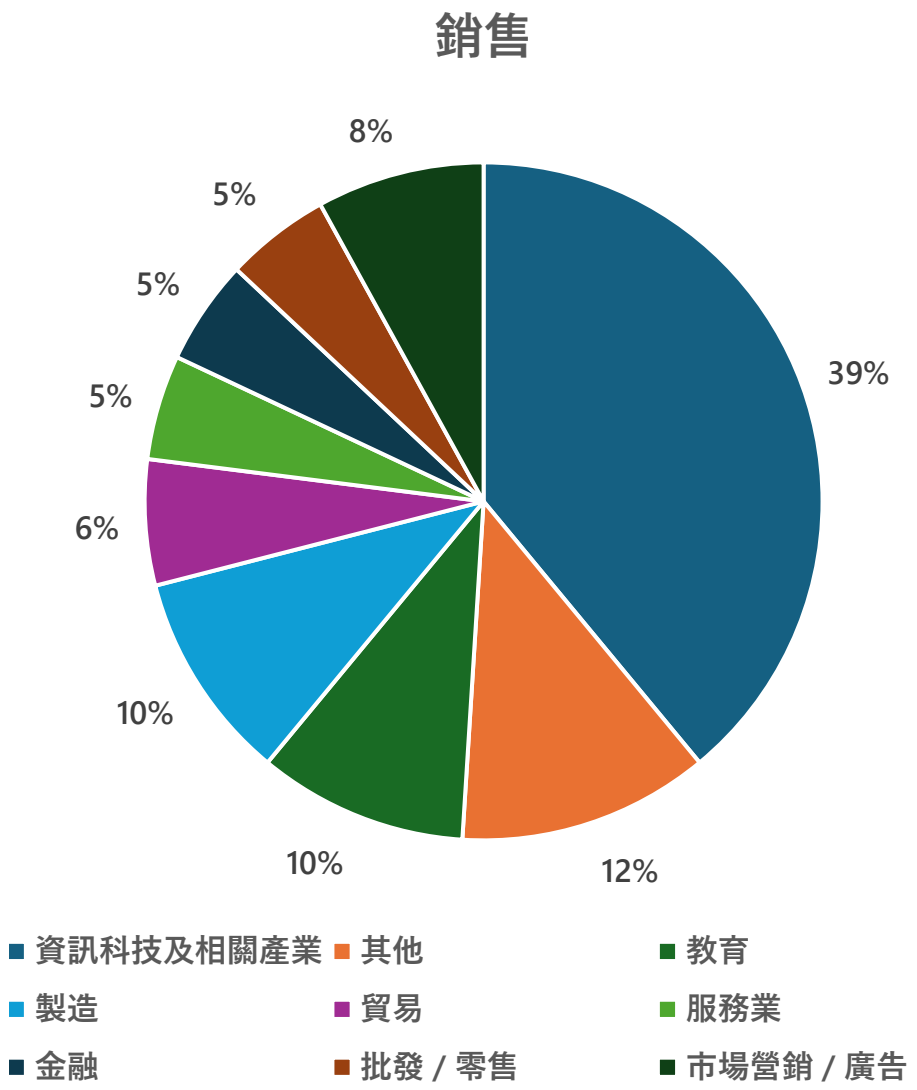
有否使用物聯網設備





調查方法

有參與是次調查的中小企受訪者當中，行業分佈主要如下:

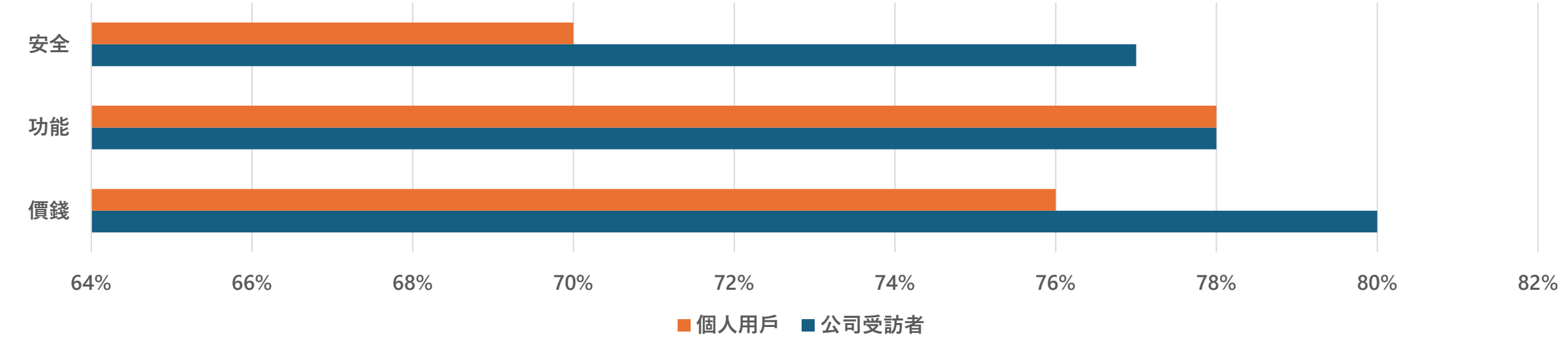


最常用的物聯網設備

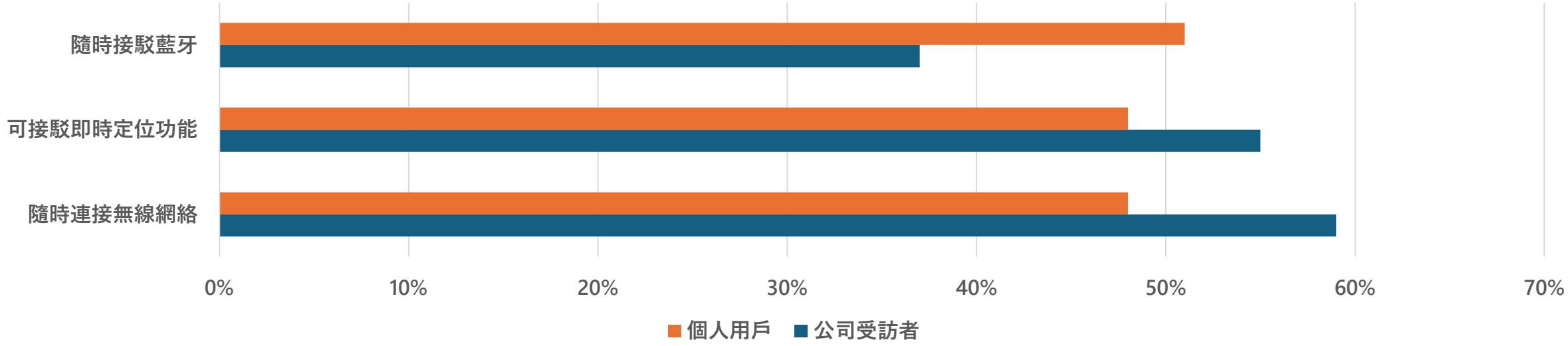
一些常見的物聯網設備包括智能手機、智慧家居裝置（如智能燈泡、智能插座、智能音箱）、智能手錶、智能車輛、智能攝像頭、智能冰箱等。這些設備能夠連接到互聯網，實現資訊交流和遠程控制，提供更便捷的生活體驗。

公司受訪者		個人用戶
74% 受訪者表示公司主要使用Wi-Fi 閉路電視/攝錄系統		41% 使用Wi-Fi 閉路電視/攝錄系統
71% 使用Wi-Fi 路由器		59% 使用Wi-Fi 路由器
42% 使用電子門鎖		
47% 使用智能手錶/手環		73% 使用智能手錶/手環
		25% 使用智能照明系統

首三個購買物聯網產品時遇到的顧慮



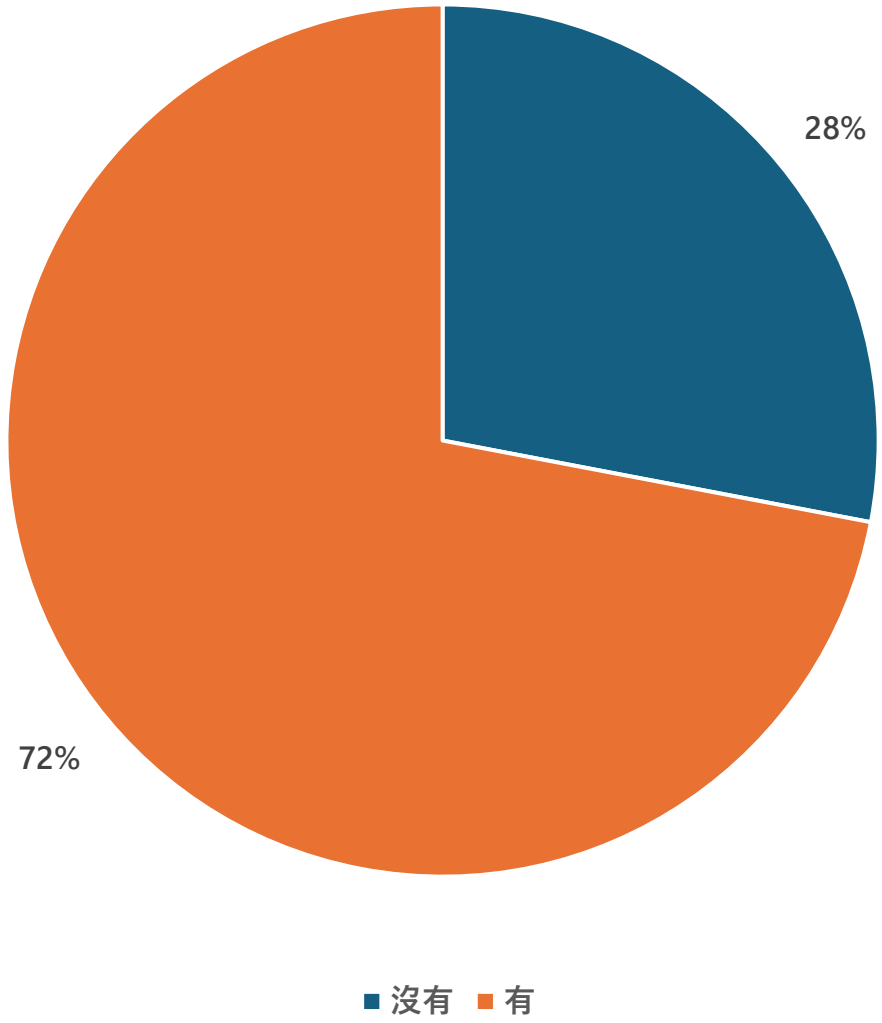
首三個受訪者認為物聯網技術最方便特點



03 使用物聯網的保安意識

公司有否管理物聯網應用風險

企業應對物聯網應用風險非常重要。公司應評估潛在的安全漏洞、隱私問題和數據風險， 並實施適當的保護措施， 如加密、身份驗證和漏洞修補。同時，建立緊急應對計劃以應對可能的攻擊和故障情況，以確保物聯網應用的安全運營。



受訪公司的資訊保安意識和政策

41%

受訪者表示公司有員工負責監督和參與物聯網及網絡安全相關的工作

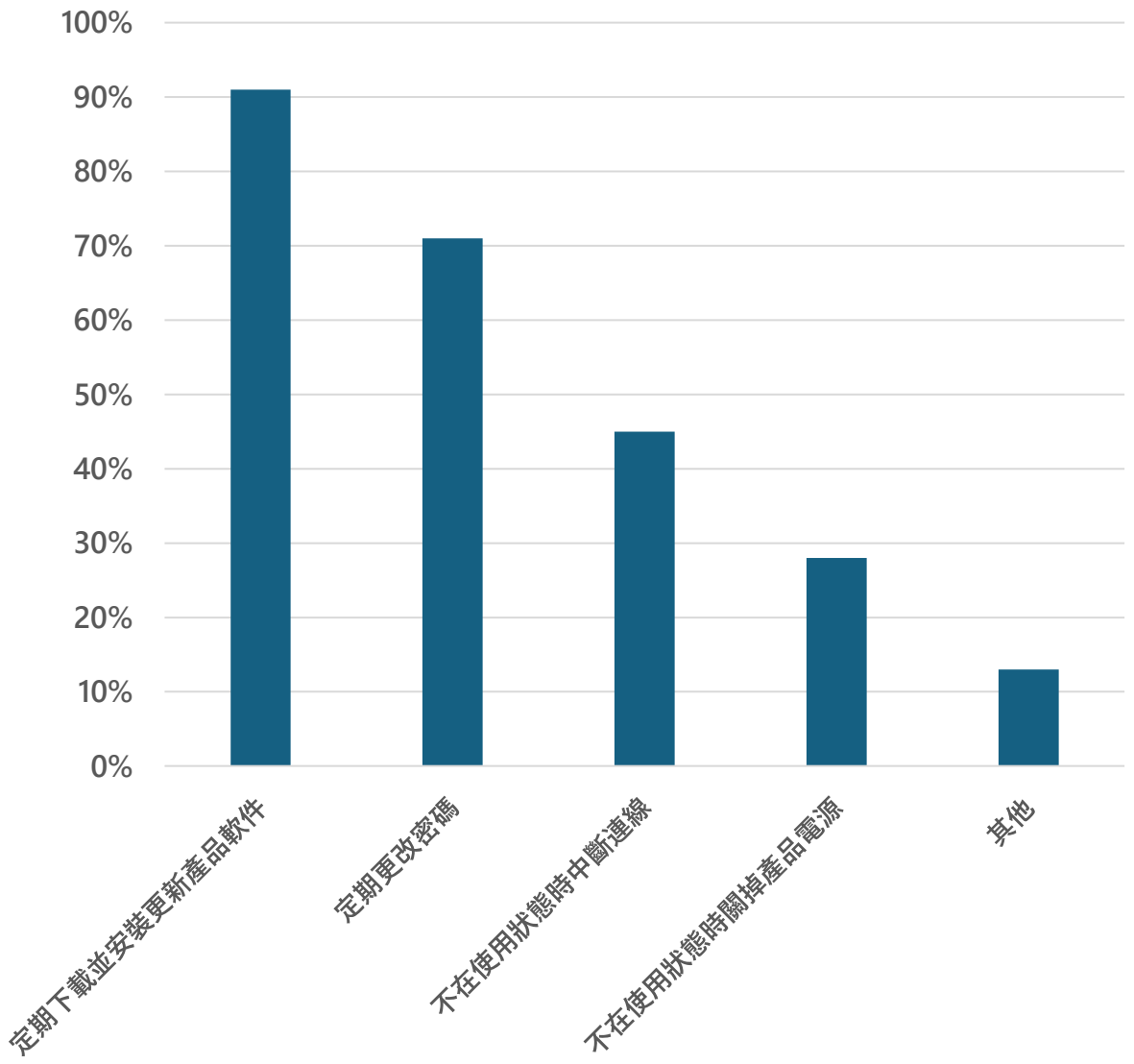
34%

受訪者表示公司已制定有關控制使用物聯網產品及其相關網絡安全問題的政策/指導方針

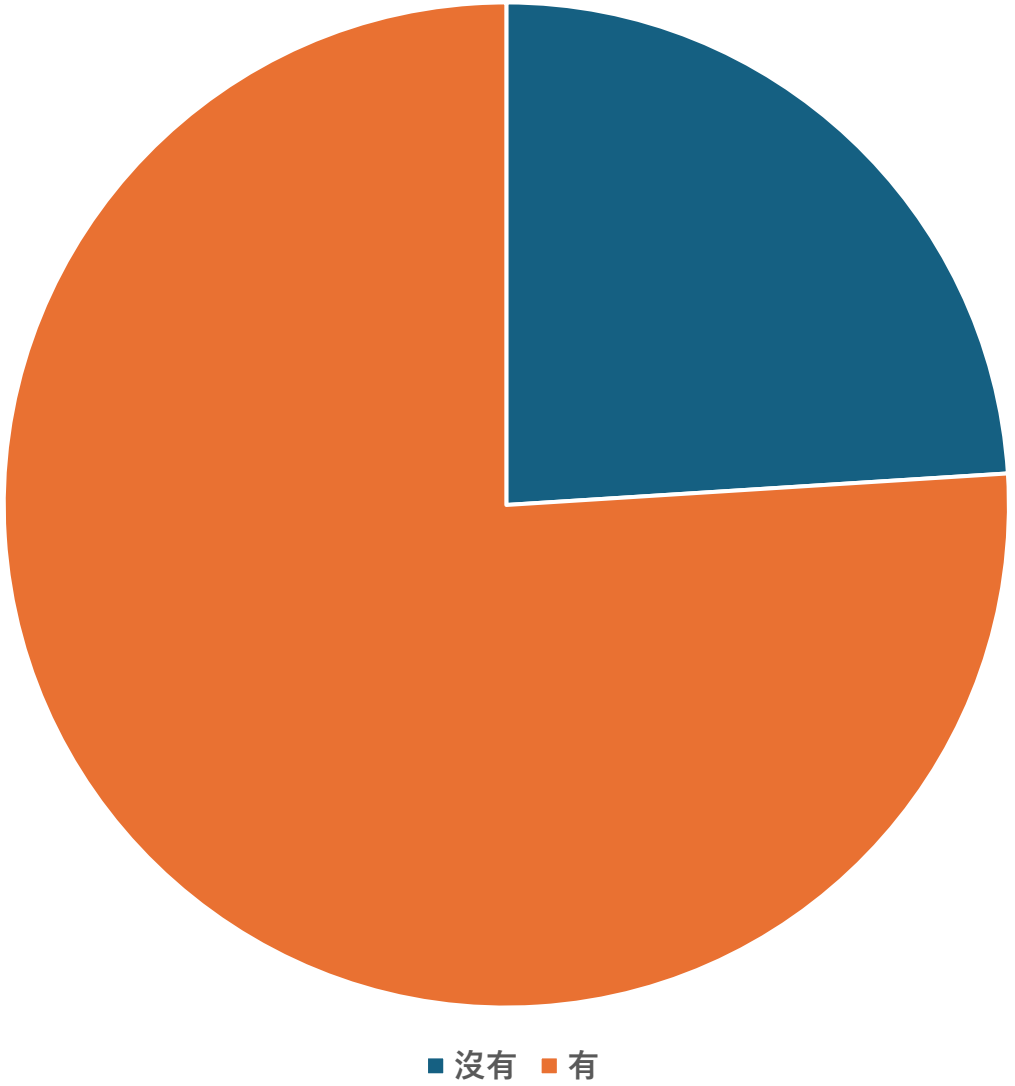
24%

受訪者表示公司每年都會為員工安排科技安全培訓

受訪公司最常降低網絡安全風險的行為



個人用戶有否管理物聯網應用風險



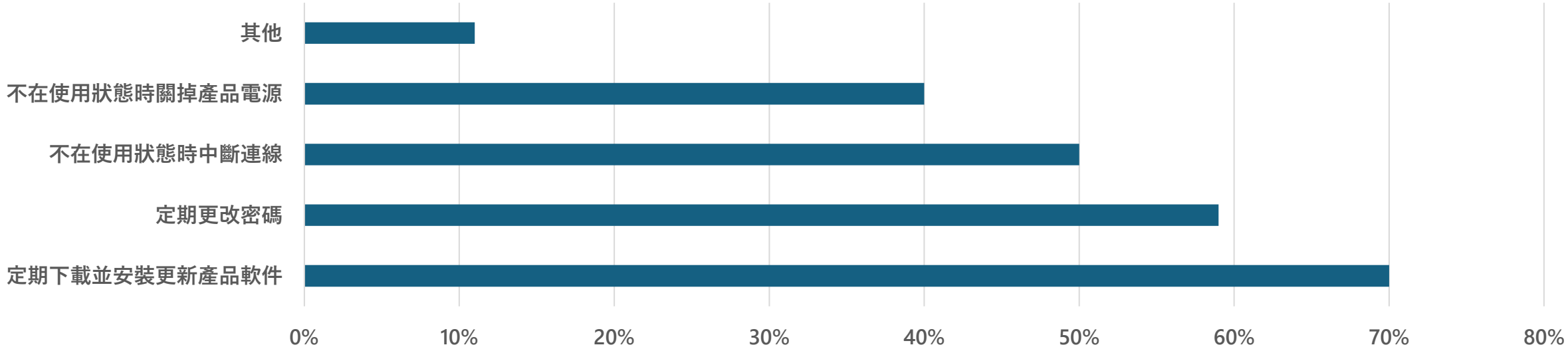
個人用戶的資訊保安意識

81% 受訪者表示會更改預設密碼

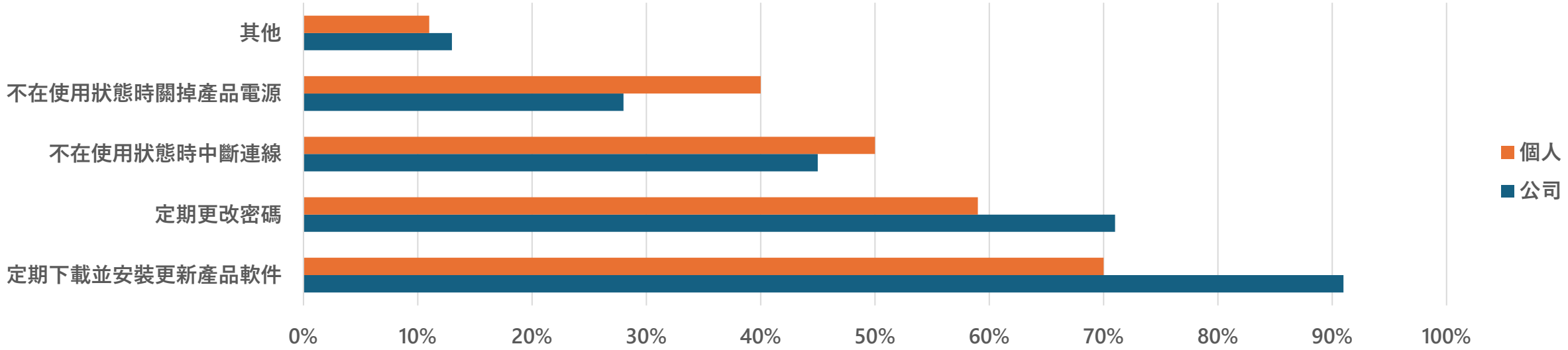
66% 受訪者表示會按照指示更新物聯網產品的軟件更新

29% 受訪者表示會閱讀物聯網產品製造商提供的條款細則

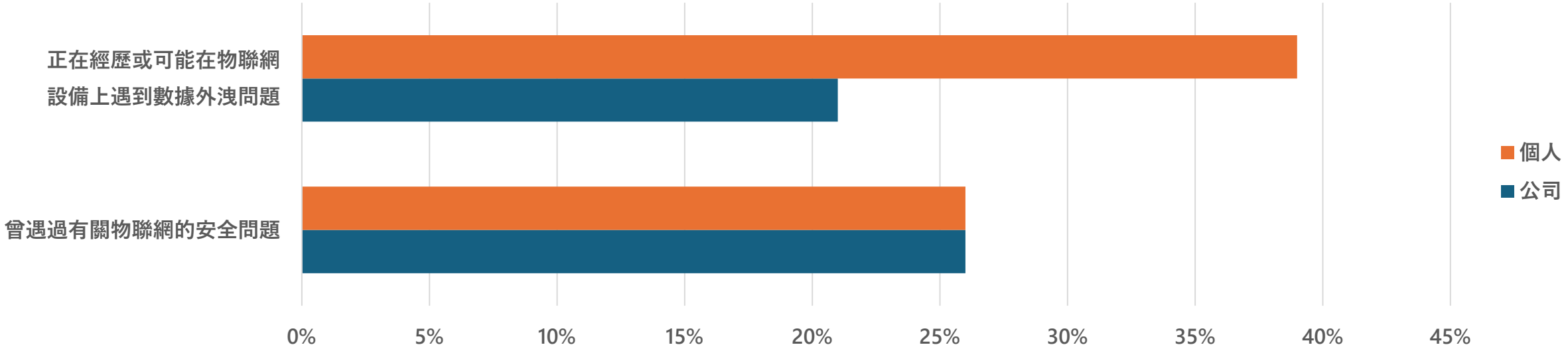
個人用戶最常降低網絡安全風險的行為



比較公司與個人受訪者最常降低網絡安全風險行為

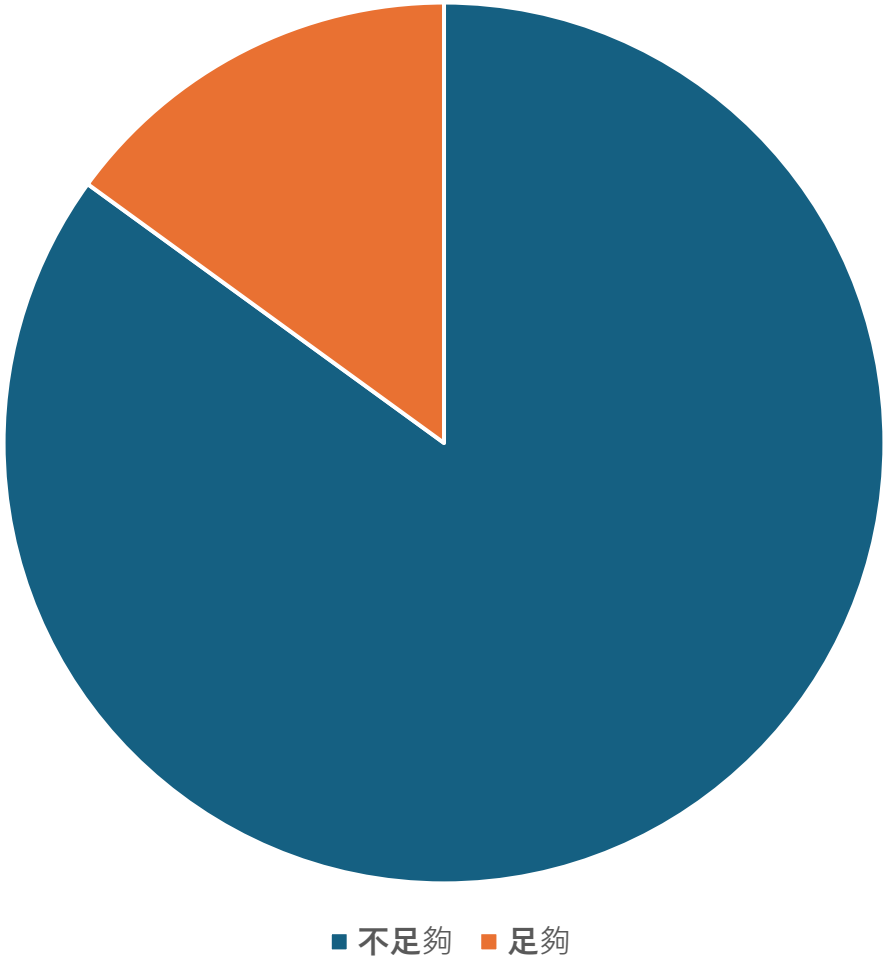


受訪者曾遇過的資訊保安問題

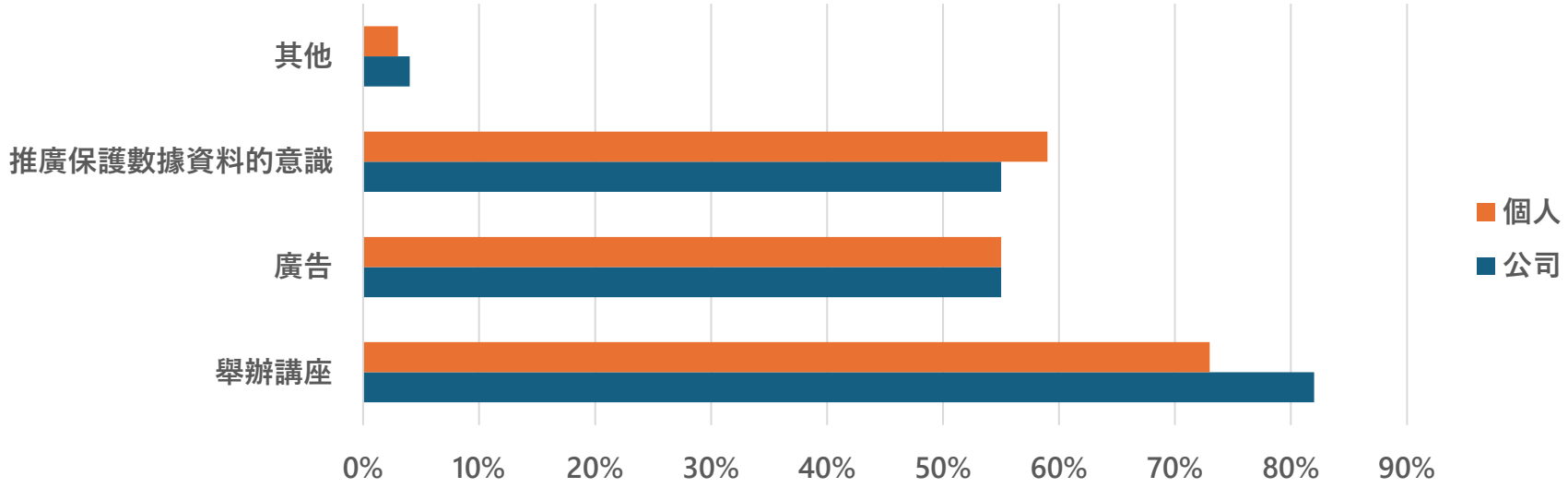


04 公眾對物聯網安全教育的看法

有關物聯網使用安全意識的公眾教育足夠嗎？



公眾對物聯網安全教育的看法



- 兩組受訪者均認為應該經常舉辦講座增加物 聯網安全知識
- 應該加強宣傳廣告提高公眾的網絡安全意識
- 受訪者認為應該加強推廣保護數據資料的重要性

總結

- 儘管大部份受訪者均有使用物聯網產品，但他們對物聯網的資訊保安意識仍有待加強。除了定期更新軟件及更改原廠密碼外，還建議：

1. 舉辦各類形式的講座及增加推廣宣傳，提高公眾對安全使用物聯網產品的意識

2. 鼓勵企業主動制定使用物聯網產品及其網絡安全問題的政策

3. 通過培訓提高公司員工的保安意識，有助提高企業的網絡安全水平

多謝

如果你有任何問題，請隨時與我們聯繫。

電子郵件：marketing_g@hkirc.hk

網址： www.hkirc.hk