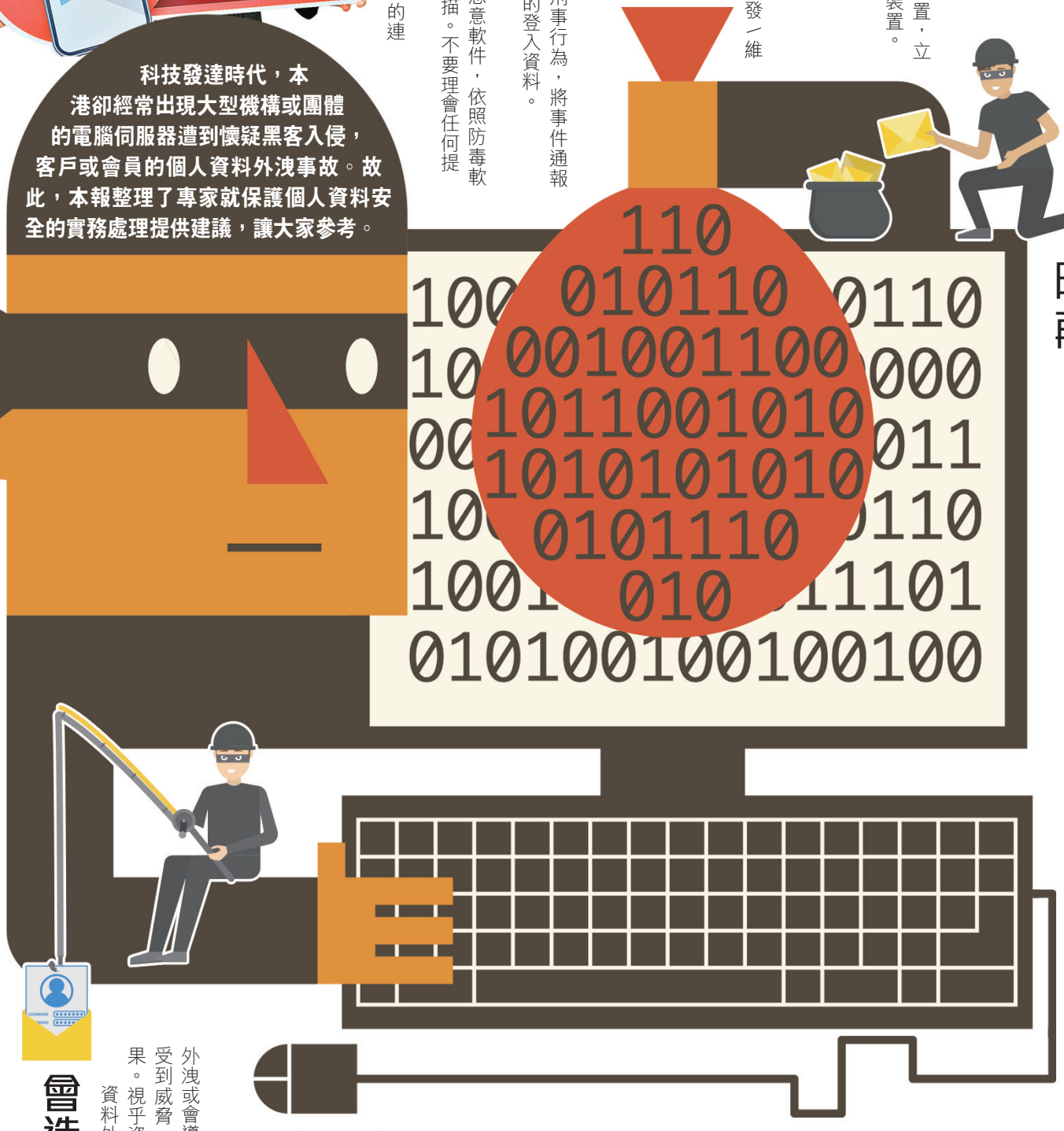
實務處理建議 資料外洩事故

■公司發生資料外洩事故，應即時通報香港私隱專員公署。

資料圖片

科技發達時代，本港卻經常出現大型機構或團體的電腦伺服器遭到懷疑黑客入侵，客戶或會員的個人資料外洩事故。故此，本報整理了專家就保護個人資料安全的實務處理提供建議，讓大家參考。



應採取什麼即時行動？

1. 立即收集資料
- 事故於何時及何地發生。
- 事故如何被發現及由誰人發現。
- 事故的肇因是什麼。
- 涉及什麼種類的個人資料及範圍有多大。
- 受影響的資料當事人有多少。

2. 評估損害
- 人身安全受到威脅。
- 身份盜竊。
- 財務損失。
- 受辱或喪失尊嚴、名譽或關係受損。
- 失去生意或聘用機會。

3. 聯絡相關人士
- 執法部門。
- 香港個人資料私隱專員公署。
  查詢熱線：2827 2827
  電郵：enquiry@pcpd.org.hk
- 互聯網公司。
- 資訊科技專家。

4. 遏止措施
- 如資料外洩是系統故障造成，應停止有關系統的操作。
- 更改用戶密碼及系統配置，以控制查閱及使用資料。
- 如犯罪活動已發生或相當可能發生，應通知有關執法部門。
- 保留資料外洩的證據以協助調查。

會造成什麼的後果？

外洩或會導致社會恐慌和危害人身安全。受到威脅。資產、健康和身份記錄等機密資料果。視乎資料外洩的程度，社會大眾有可能會資料外洩可能會對機構和個人造成嚴重後

機構財務損失：資料外洩可能會影響或破壞機構的日常運作，導致業務上的損失。其他財務後果包括收入減少、知識產權損失(例如專利和商業秘密)、支付和解費用，並且要支付法律服務、應對外洩情況和調查費用等。

法律後果：不同地區均已實施有關資料外洩影響的客戶作出補償及會面對監管機構的法律行動(例如罰款和訴訟)。

聲譽損害：資料外洩會嚴重損害機構的聲譽。商業信譽受到損害將對品牌形象造成負面影響，並失去客戶的信任，以及影響與商業夥伴或供應商的關係。

身份盜竊：可識別個人身份的敏感資料，冒充當事人進行其他惡意活動，例如非法轉移受害者的資金及利用受害者的身份進行欺詐。

個人資料外洩會對個人造成嚴重影響。攻擊者使用以欺詐方式獲得的登入憑證進行欺詐。

遺失實體文件或便攜裝置

即時處理方法：
- 若無法尋回遺失的文件／便攜式儲存裝置，立即通知資料當事人。
- 盡快嘗試尋找遺失的文件／便攜式儲存裝置。

不當／錯誤地處置個人資料

即時處理方法：
- 若發生或有可能發生刑事行為，將事件通報相關的執法部門。
- 停用有關員工的賬戶／存取權限。

不慎以電郵或郵寄披露

即時處理方法：
- 若未能回收／取回有關電郵／信件，立即通知並要求非預期的收件者刪除有關電郵／銷毀有關信件。
- 在可行的情況下，嘗試回收／取回有關電郵／信件。

網絡攻擊

即時處理方法：
- 切斷被入侵的裝置與互聯網及其他網絡的連接。
- 切斷有關程式／系統／平台的存取連接。
- 若有關程式／系統／平台由第三者開發／維護，立即聯絡負責的供應商。
- 若發生或有可能發生身份盜竊或其他刑事行為，將事件通報相關的執法部門。
- 更改被入侵的裝置／軟件／資料庫／系統的登入資料。
- 示你連接互聯網的訊息，若發現任何惡意軟件，依照防毒軟使用防毒軟件為離線的電腦網絡進行掃描。不要理會任何提

系統錯置

即時處理方法：
- 若發生或有可能發生身份盜竊或其他刑事行為，將事件通報
- 更改被入侵的裝置／軟件／資料庫／系統的登入資料。

防止事故再次發生建議

- 改善個人資料處理程序中的保安問題。
- 限制授予個別人士查閱及使用個人資料的查閱權。應遵守有需要知道及有需要查閱的原則。
- 現有資訊科技保安措施是否足以保障個人資料免受黑客入侵、未經准許的或意外的查閱、處理、刪除、喪失或使用。
- 因應資料外洩事故而修改或制訂相關的私隱政策及措施。
- 如何有效偵測資料外洩事故。保存適當的查閱紀錄有助察覺早前警號。
- 加強對僱員、代理及資料處理者的監察及監督機制。
- 提供在職培訓，以推廣私隱意識及提高處理個人資料的僱員的良好操守、審慎態度及辦事能力。聘用資料處理者的政策和檢討與資料處理者簽訂的合約中有關保障個人資料私隱的條款，包括規定資料處理者立即通報任何資料外洩事件。