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

「應對網絡安全威脅及資料外洩事故」講座

譚嘉榮
個人資料主任（資訊科技）

2024年5月10日

數據安全的重要性


etnet
消費者委員會
CONSUMER COUNCIL
消委會遭黑客入侵
料員工及月刊訂戶資料外洩
拒交50萬美元贖金


ezone
數碼港
Cyberport
數碼港遭黑客入侵
疑洩 400GB 數據涉敏感個人資料


hket
香港經濟日報
香港銀行學會
The Hong Kong Institute of Bankers
暫停部分電子服務
遭勒索軟件攻擊
香港銀行學會：會員資料有被洩露風險


星島頭條
快圖美
FOTOMAX
洩54萬會員
及7萬客戶私隱
快圖美被揭1年多前
已知保安漏洞拒修補

《私隱條例》的相關規定

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

《私隱條例》的規定 — *1) 有關資料保安的規定*

保障資料第4原則

資料使用者須採取**所有切實可行的步驟**，以確保由資料使用者持有的個人資料受保障，而不受**未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響**。

NOTE

在發生資料外洩的情況下，資料使用者有責任證明他們已採取**所有合理地切實可行的步驟**保障個人資料的安全，而「合理地切實可行」的步驟將視乎每個個案的案情而定。

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

數據安全建議措施

下載小冊子

下載指引

資訊及通訊科技的數據安全建議措施

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

資料管治和機構性措施 *政策及程序*

資料使用者應制訂明確針對資料管治和資料保安的內部政策和程序，並涵蓋:

- 角色和責任
- 資料的查閱和輸出
- 應付事故
- 風險評估
- 外判工作
- 銷毀資料

NOTE

資料使用者應根據當時情況（如業內新標準、資料保安新威脅等），定期和及時地覆檢與修訂政策及程序。

資訊及通訊科技的數據安全建議措施

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

資料管治和機構性措施 *培訓*

工作人員應在入職時及往後**定期接受足夠培訓**，培訓類型可包括:

NOTE

企業可考慮將「**演習**」納入資料保安培訓，以提高員工的警覺程度，建立一道「**人力防火牆**」

資訊及通訊科技的數據安全建議措施

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

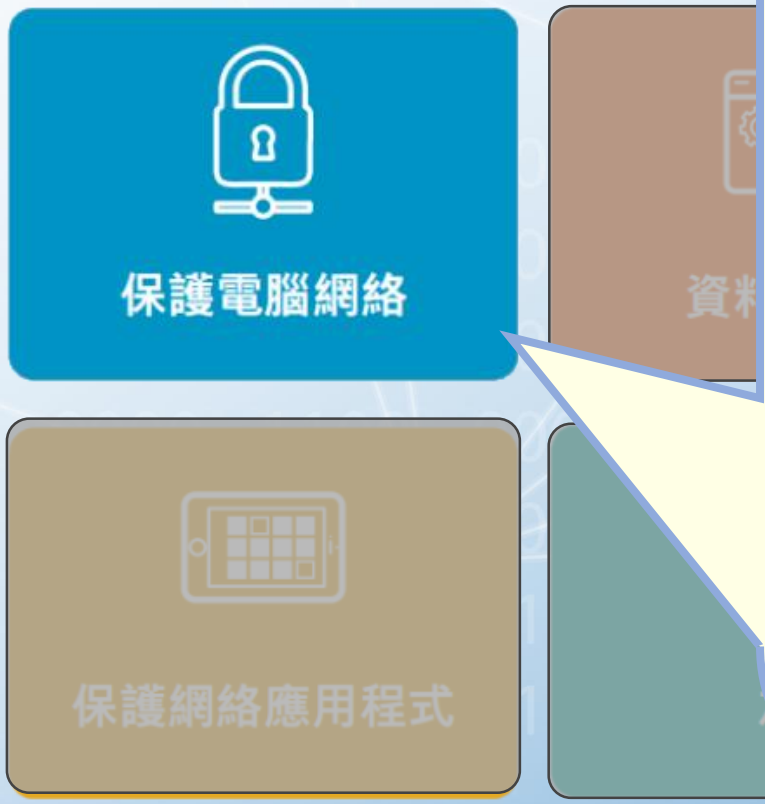
技術上及操作上的保安措施

- 保護電腦網絡
- 資料庫管理
- 存取管控
- 防火牆和反惡意軟件
- 保護網絡應用程式
- 加密
- 電郵及檔案傳送
- 資料備份、銷毀及匿名化

資訊及通訊科技的數據安全建議措施

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

技術上及操作上的保安措施

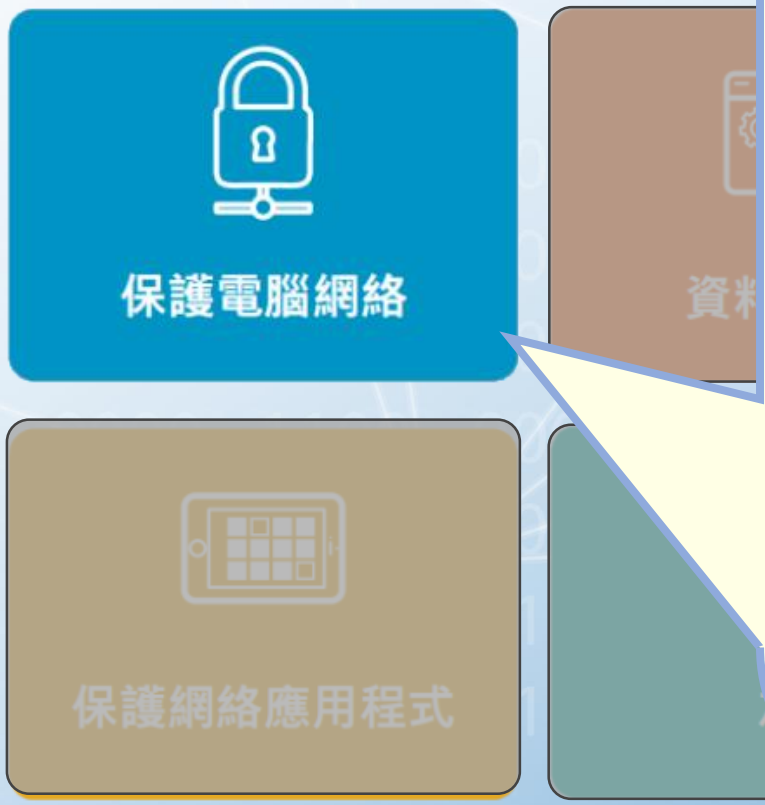


- 在網絡安裝**防火牆**，以防止未經許可的網絡連接，亦可偵測網絡攻擊
- 在電腦及伺服器安裝**防毒軟件**（反惡意軟件），以偵測及防止病毒及威脅
- 定期進行**保安漏洞評估**及**滲透測試**
- 使用**網站安全掃描服務**，定期掃描以偵測最新的已知或潛在的網絡安全風險 (*https://www.hkirc.hk/zh-hant/public_mission/cybersecurity/free_web_scan_services/*)
- 及時更新正在使用的系統及軟件，可以**修補保安漏洞**，減少被攻擊的機會

資訊及通訊科技的數據安全建議措施

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

技術上及操作上的保安措施



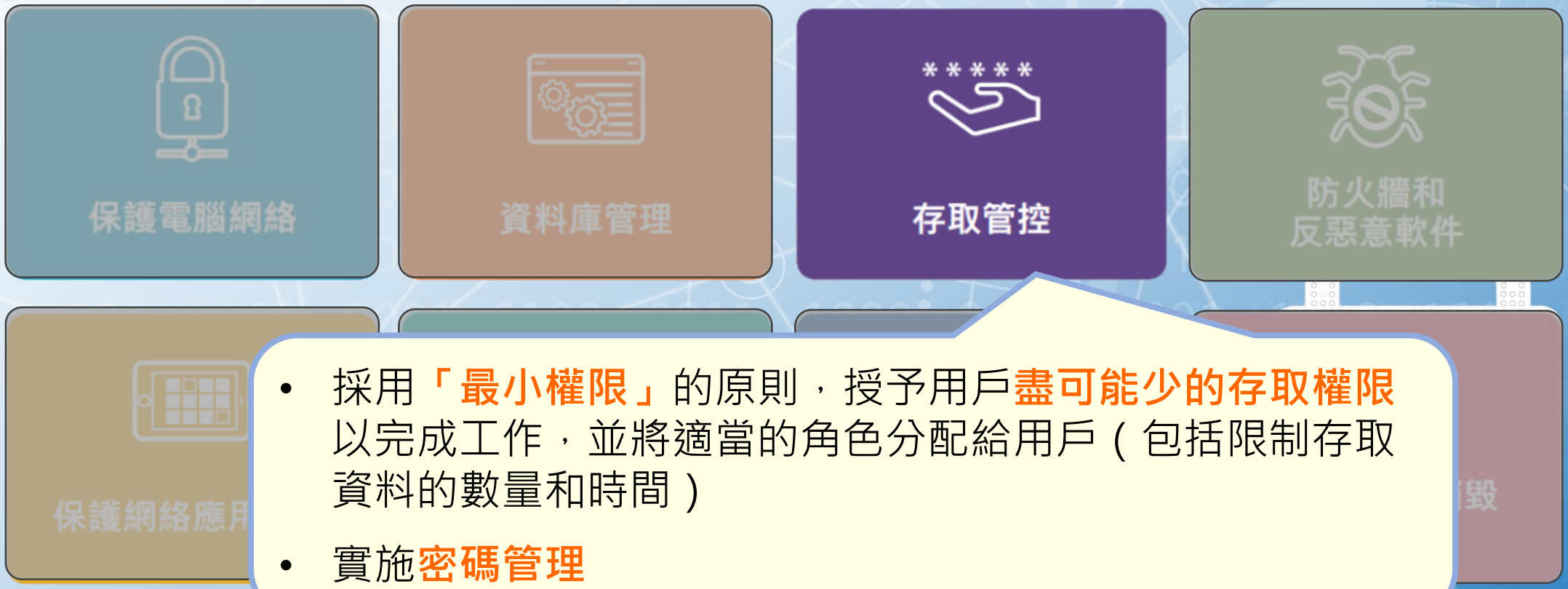
最新網絡威脅資訊：

- 守網者
  https://cyberdefender.hk/
- 網絡安全資訊共享夥伴計劃
  https://www.cybersechub.hk/
- 香港電腦保安事故協調中心
  https://www.hkcert.org/

資訊及通訊科技的數據安全建議措施

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

技術上及操作上的保安措施



- 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）
- 實施**密碼管理**

資訊及通訊科技的數據安全建議措施

技術上及操作上的保安措施

- 網站**使用HTTPS**（SSL Certificate）可以加密傳輸中的資料
- 使用有加密功能的USB存儲資料
- 為機密文件（Word / Excel）加上**密碼**

資訊及通訊科技的數據安全建議措施

NOTE

根據《私隱條例》第65(2)條，資料使用者須對其代理人（包括資料處理者）的行為負責

資料處理者的管理

資料使用者在聘用資料處理者時可考慮：

- 實施政策及程序確保**只聘用稱職且可靠**的資料處理者
- 進行評估**確保只有必要的個人資料轉移**至資料處理者
- 於合同**明確規定**資料處理者須採取的**保安措施**
- 要求資料處理者在發生資料保安事故時**立即作出通知**
- **進行現場審核**以確保資料處理者遵守資料處理合同的要求

資料外洩事故處理

保障、尊重個人資料私隱
Protect, Respect Personal Data Privacy

主頁 > 審查及執法 > 資料外洩事故通報

資料外洩事故通報

資料外洩事故一般指資料使用者持有的個人資料懷疑外洩，令此等資料承受遺失或未獲准許的或意外的查閱、處理、刪除或使用的風險。

雖然法例沒有規定資料使用者就他們持有的個人資料的外洩事故通知私隱專員公署，但私隱專員公署建議資料使用者作出通報，以妥善處理有關事故。你可在提交資料外洩事故通報前，參考私隱專員公署的《資料外洩事故的處理及通報指引》。

私隱專員公署鼓勵資料使用者使用網上資料外洩事故通報表格通報資料外洩事故。請按此查閱網上資料外洩事故通報表格。

除網上表格外，資料使用者仍可下載紙本資料外洩事故通報表格，以供填寫。請按此下載紙本資料外洩事故通報表格。填妥表格後，你可透過以下途徑把表格及其他與資料外洩事故相關的文件（如有）一併遞交。

- **親臨私隱專員公署或郵寄**

  地址:
  香港灣仔皇后大道東248號大新金融中心13樓1303室

  私隱專員公署接待處辦公時間:
  星期一至星期五：
  上午8時45分 至 下午12時45分
  下午1時50分 至 下午5時40分

- **傳真**
  傳真號碼:28777026

- **電子郵遞**
  電郵地址:dbn@pcpd.org.hk

資料外洩事故處理

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

「事故發生前」—資料外洩事故應變計劃

- 載列機構一旦發生資料外洩時會**如何應對的文件**
- 有助機構快速應對及有效管理事故
- 資料外洩事故應變計劃應：
  - ① 概述發生事故後**須執行的程序**
  - ② 資料使用者由事故開始到完結就**識別**、**遏止**、**評估**以至**管理**事故所帶來的影響的策略
- 計劃主要涵蓋範疇包括：外洩事故的**定義**、**通報**程序、應變小組的**角色及責任**、**風險評估**工作流程、**遏止**策略、**調查**程序、**紀錄**政策、事後**檢討**機制、**培訓或演習**計劃等

資料外洩事故處理

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

「事故發生後」－處理資料外洩事故5大步驟

步驟 1 ：立即收集重要資料

資料使用者必須**迅速收集事故的所有相關資料**，以評估對資料當事人的影響及找出適當的緩和措施，包括：

- 事故於**何時及哪裏**發生？
- 事故**如何被發現**及由**誰人發現**？
- 導致事故的**原因**是甚麼？
- 涉及**甚麼種類**的個人資料？
- **有多少個**可能受影響的資料當事人？
- 可能對受影響人士造成甚麼**傷害**？

NOTE

最先發現事故的職員應考慮是否依從資料外洩事故應變計劃所訂的程序向專責應變小組／高級管理層／保障資料主任通報事故

資料外洩事故處理

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

步驟 2：遏止事件擴大

機構可視乎所涉及個人資料的類別及事故的嚴重性，考慮採取以下的遏止措施：

- 要求錯誤接收有關電郵 / 信件 / 傳真的人士**銷毀或交回誤發的文件**
- **關閉或隔離**受損 / 遭破壞的系統 / 伺服器
- **修復**導致事故的**漏洞或錯誤**
- **更改用戶密碼及系統配置**
- **移除**涉嫌造成或引致資料外洩的**用戶的查閱權**
- 如已發生或可能發生身分盜竊或其他犯罪活動，應**通知有關執法部門**

資料外洩事故處理

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

步驟 3：評估事件可造成的損害

資料外洩事故可導致的損害包括：

- 人身安全受到威脅
- 身分盜竊
- 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

因資料外洩而可能蒙受的傷害程度取決於：

例如：

- 外洩個人資料的**種類**、**敏感程度**及**數量**
- 資料外洩的情況
- 傷害的性質
- **身分盜竊**或**詐騙**的可能性
- 遺失的資料**有否備份**
- 外洩資料有否進行足夠的**加密**、**匿名化**或其他保障措施
- 資料外洩**持續的時間**

資料外洩事故處理

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

步驟 4：考慮作出資料外洩通報

資料使用者在決定是否把事故通知受影響資料當事人、私隱專員公署及其他執法部門時，應考慮：

- 事故可能對受影響人士**造成的影響**
- 影響**有多嚴重**或重大
- 發生的**可能性**
- **不作出通知的後果**

NOTE

如資料外洩事故相當可能對受影響資料當事人有構成實質傷害的風險，資料使用者應在知道發生資料外洩後在切實可行的情況下盡快通知私隱專員公署及受影響資料當事人

資料外洩事故處理

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

步驟 5：記錄事故

- 資料使用者必須**完整地記錄事故**，包括事故的**詳情、影響，資料使用者所採取的遏止措施和補救行動**
- 機構如須依從其他司法管轄區的法例及規例，亦應留意有關法例及規例下的**強制記錄要求**

NOTE

例如歐洲聯盟的《通用數據保障條例》規定資料控制者記錄所有資料外洩事故並保存有關紀錄


資料外洩事故的
處理及通報指引
PCPD.org.hk
香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

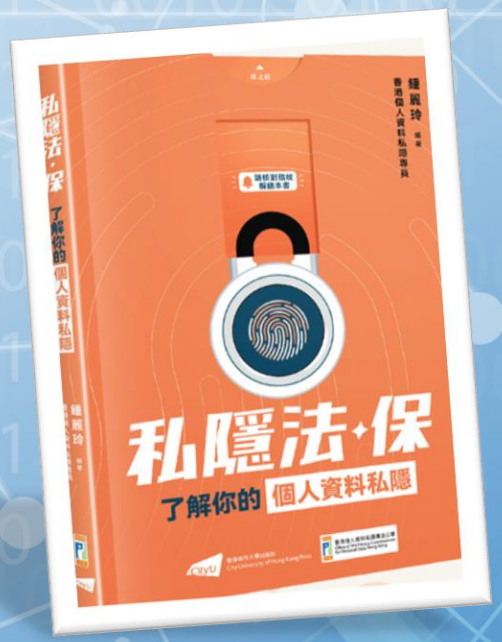
下載指引

下載小冊子

其他資訊科技相關指引及資料單張

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

- 《電子點餐的私隱關注》報告
- 《數碼時代的私隱保障：比較十大網購平台的私隱設定》
- 社交媒體私隱設定大檢閱
- 開發及使用人工智能道德標準指引 – 指引資料
- 保障個人資料私隱 – 使用社交媒體及即時通訊軟件的指引
- 保護你的數碼身分
- 資訊及通訊科技系統的貫徹數據保障設計指引
- 經互聯網收集及使用個人資料：以兒童為對象的資料使用者注意事項
- 開發流動應用程式最佳行事方式指引
- 使用便攜式儲存裝置指引
- 經互聯網收集及使用個人資料：給資料使用者的指引
- 個人資料的刪除與匿名化指引



編著:
鍾麗玲
私隱專員

訂購表格

PCPD.org.hk

PCPD HK

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

數據安全熱線
Data Security Hotline
2110 1155

數據安全快測
Data Security Scanner
https://www.pcpd.org.hk/Toolkit/tc/

數據安全專題網頁
Data Security Webpage
https://www.pcpd.org.hk/tc_chi/data_security/index.html

謝謝！Thank you!