「認識《保護關鍵基礎設施（電腦系統）條例》與數據安全」研討會

預防及處理資料外洩事故
及
提升機構網絡安全的建議措施

鍾麗玲女士
個人資料私隱專員

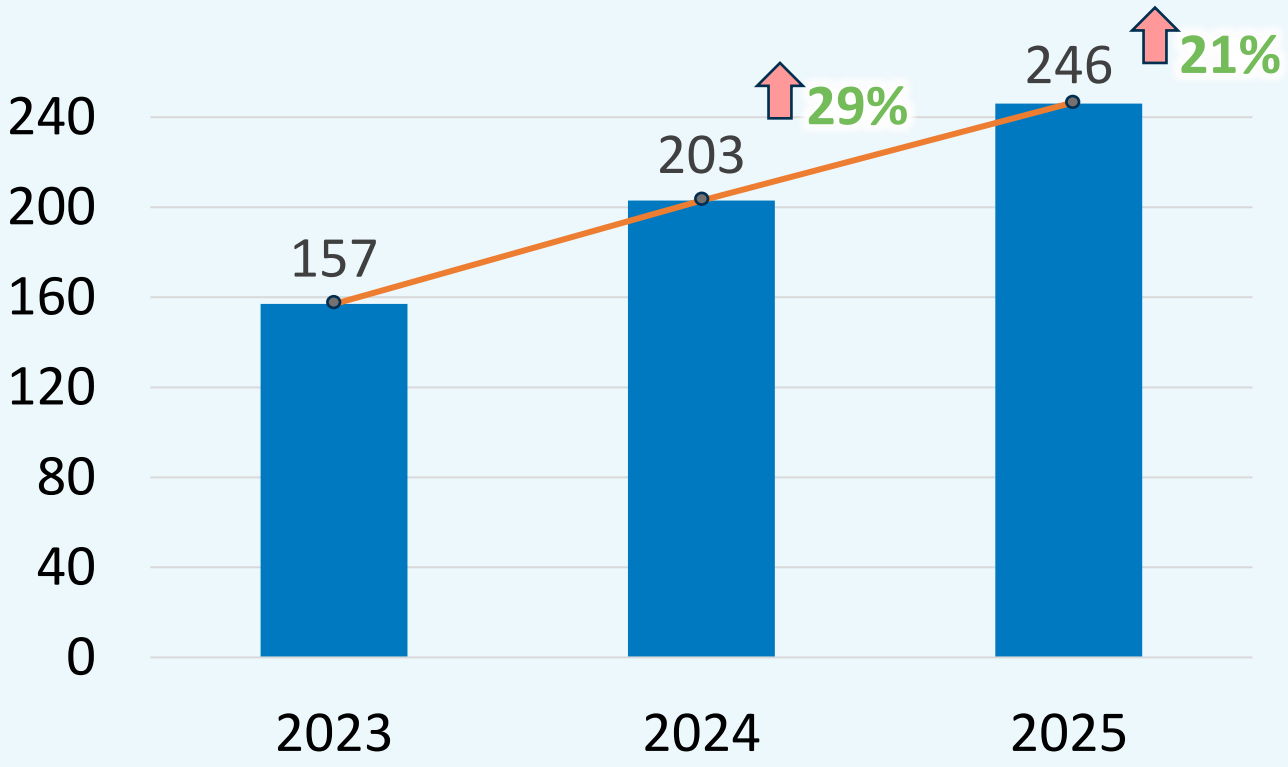
2026年2月5日

守護私隱・改革創新 Protecting Privacy · Embracing Innovation

PCPD.org.hk
個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data
中國香港 Hong Kong, China

個人資料外洩事故

2025年資料外洩事故通報數字

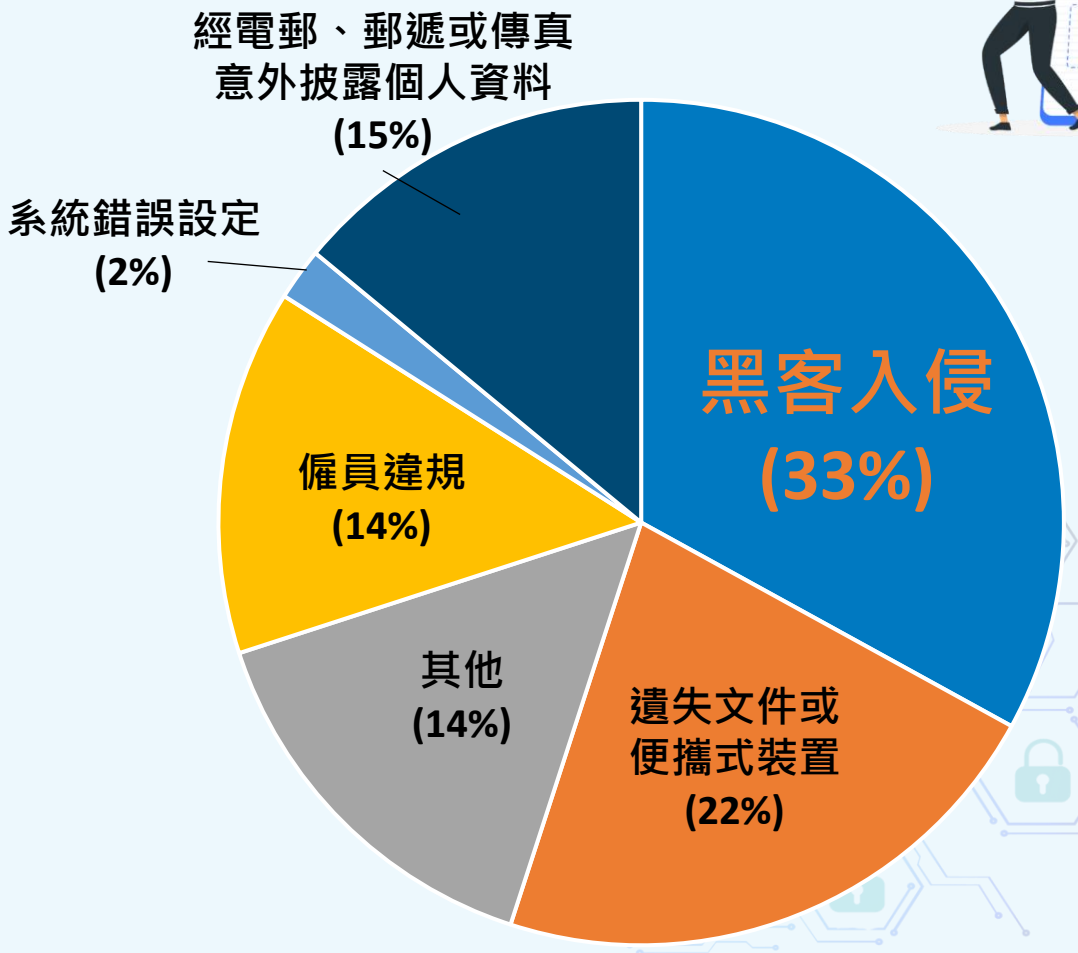


- 在2025年，私隱專員公署接獲246宗資料外洩事故通報（79宗來自公營機構及167宗來自私營機構），較2024年的203宗增加21%

個人資料外洩事故

2025年資料外洩事故分類

- 在2025年私隱專員公署接獲的資料外洩事故通報中，81宗涉及黑客入侵，佔整體資料外洩事故通報的33%



《私隱條例》的相關規定

資料外洩事故可構成違反《私隱條例》附表1的保障資料第4原則

保障資料第4(1)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

保障資料第4(2)原則

如資料使用者聘用（不論是在香港或香港以外聘用）**資料處理者**，以代該資料使用者處理個人資料，該資料使用者須採取**合約規範方法**或其他方法，以防止轉移予該資料處理者作處理的個人資料未獲准許或意外地被查閱、處理、刪除、喪失或使用

《個人資料（私隱）條例》及《保護關鍵基礎設施（電腦系統）條例》的規管對象

《個人資料（私隱）條例》

《保護關鍵基礎設施（電腦系統）條例》

其他營運者

關鍵基礎設施營運者


個案分享

個案（1）

一間非牟利機構的資訊系統遭受勒索軟件攻擊

背景

黑客透過**暴力攻擊**及利用**防火牆的嚴重漏洞**，**控制**一個資訊科技測試人員**帳戶**，並識別出網絡中**存有漏洞的伺服器**，繼而取得活動目錄的**管理員權限**。黑客隨後進行**橫向移動**，入侵機構的伺服器、工作電腦及手提電腦，並在資訊系統放置勒索軟件，導致儲存在系統內的檔案及資料被加密及竊取。

受是次外洩事件影響的人士約 **550,000名**。

缺失

1. 過時的防火牆存在嚴重漏洞
2. 未有啟用多重認證功能
3. 沒有對伺服器進行關鍵保安修補
4. 資訊系統欠缺有效的偵測措施
5. 對資訊系統進行的保安評估不足
6. 資訊保安政策有欠具體
7. 過長地保存個人資料

個案（2）

兩間零售及批發公司的資訊系統遭黑客入侵

背景

兩間公司的資訊系統遭黑客利用**暴力攻擊**，獲取了**具系統管理員權限帳戶的帳戶憑證**，並在資訊系統進行**橫向移動**，包括於一台用於內部系統開發及編程的桌上電腦**注入木馬程式**，繼而獲取能**操控資料庫伺服器**的**原始程式碼**，並盜取及刪除儲存在內的個人資料。

受是次外洩事件影響的客戶及員工約 **79,400名**。

缺失

1. **未有適時刪除離職員工帳戶**
2. **資訊系統欠缺有效的保安及偵測措施**
3. **伺服器的作業系統已過時**
4. **欠缺資訊保安政策及指引**
5. **未有對資訊系統進行保安評估及審計**

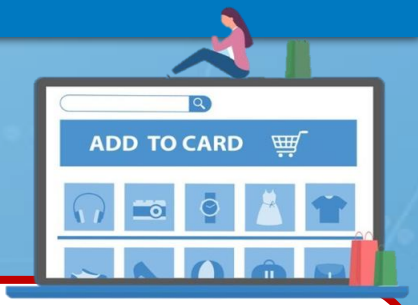
個案（3）

一間零售公司的客戶關係管理平台及電子商務平台遭受未獲授權的第三方入侵

背景

一間零售公司的**客戶關係管理平台**及**電子商務平台**遭受未獲授權的第三方入侵，導致客戶的個人資料被竊取。黑客**利用一名現職員工的管理員帳戶的帳戶憑證**，從一個不明的**海外 IP 位址連接至受影響平台**，繼而下載儲存於當中的訂單資料。受是次外洩事故影響的客戶約**59,205名**。

在調查過程中，該公司發現**受影響的個人資料**於是次外洩事件發生約兩個月後**在「暗網」公開**，並可供下載。



缺失

1. **薄弱的密碼管理**
2. **未有為存取帳戶啟用多重認證功能**
3. **缺乏保障個人資料的意識**
4. **未有對受影響平台進行適當的保安檢視**

處理資料外洩事故

資料外洩事故應變計劃

資料外洩事故應變計劃是載列機構一旦發生資料外洩時會**如何應對的文件**。一套全面的資料外洩事故應變計劃有助機構**快速應對及有效管理事故**。

資料外洩事故應變計劃應：

- 概述發生事故後**須執行的程序**
- 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

如何處理資料外洩事故

1. 立即收集重要資料
2. 遏止事件擴大
3. 評估事件可造成的損害
4. 考慮作出資料外洩通報
5. 記錄事故

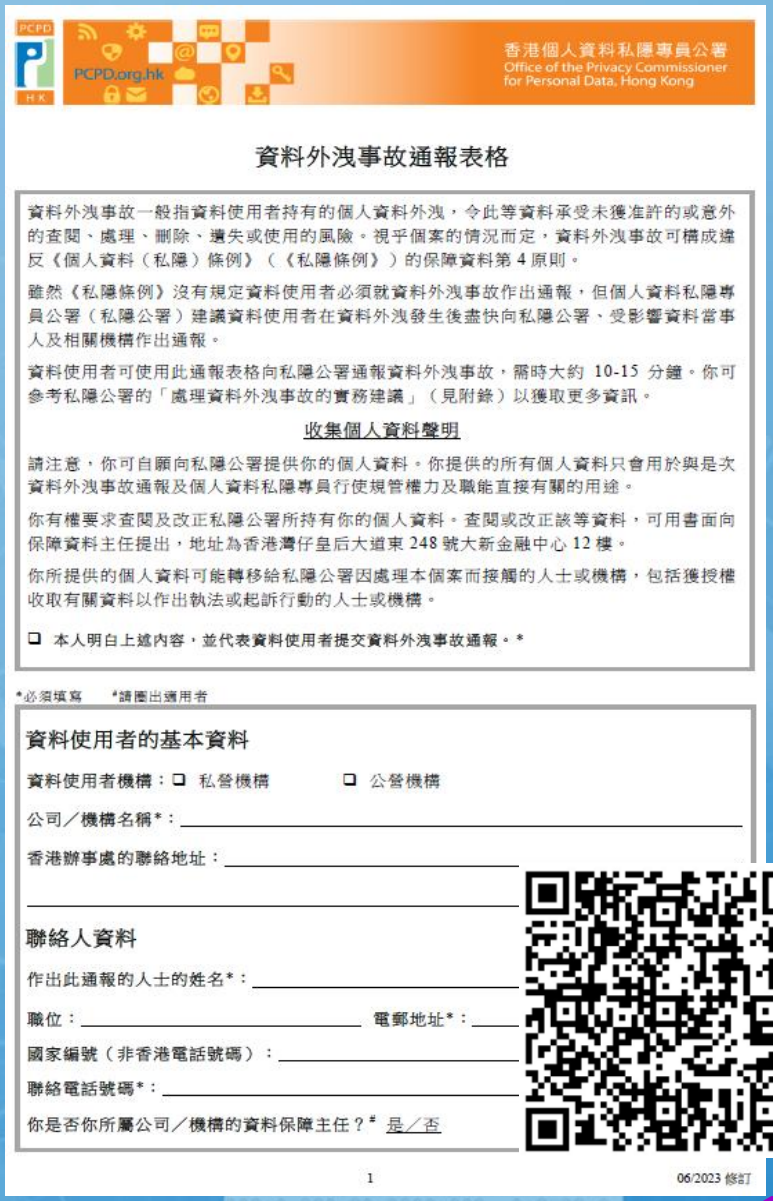
如何通報資料外洩事故

通知資料當事人

- 透過電話、書面、電郵或親身向資料當事人作出通報
- 如直接的資料外洩通報不切實可行，可發出公告、報章廣告，或於網站或社交媒體平台發出帖文

通知私隱專員公署

- 經私隱專員公署網頁、傳真、親身或以郵寄方式遞交「資料外洩事故通報表格」
- 不接受口頭通報



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

資料外洩事故通報表格

資料外洩事故一般指資料使用者持有的個人資料外洩，令此等資料承受未獲准許的或意外的查閱、處理、刪除、遺失或使用的風險。視乎個案的情況而定，資料外洩事故可構成違反《個人資料（私隱）條例》（《私隱條例》）的保障資料第 4 原則。

雖然《私隱條例》沒有規定資料使用者必須就資料外洩事故作出通報，但個人資料私隱專員公署（私隱公署）建議資料使用者在資料外洩發生後盡快向私隱公署、受影響資料當事人及相關機構作出通報。

資料使用者可使用此通報表格向私隱公署通報資料外洩事故，需時大約 10-15 分鐘。你可參考私隱公署的「處理資料外洩事故的實務建議」（見附錄）以獲取更多資訊。

收集個人資料聲明

請注意，你可自願向私隱公署提供你的個人資料。你提供的所有個人資料只會用於與是次資料外洩事故通報及個人資料私隱專員行使規管權力及職能直接有關的用途。

你有權要求查閱及改正私隱公署所持有你的個人資料。查閱或改正該等資料，可用書面向保障資料主任提出，地址為香港灣仔皇后大道東 248 號大新金融中心 12 樓。

你所提供的個人資料可能轉移給私隱公署因處理本個案而接觸的人士或機構，包括獲授權收取有關資料以作出執法或起訴行動的人士或機構。

❑ 本人明白上述內容，並代表資料使用者提交資料外洩事故通報。*

*必須填寫　#請圈出適用者

資料使用者的基本資料

資料使用者機構：❑ 私營機構　❑ 公營機構

公司／機構名稱*：

香港辦事處的聯絡地址：

聯絡人資料

作出此通報的人士的姓名*：

職位：　電郵地址*：

國家編號（非香港電話號碼）：

聯絡電話號碼*：

你是否你所屬公司／機構的資料保障主任？# 是／否

1　06/2023 修訂

網絡安全建議措施

《資訊及通訊科技的保安措施指引》

1.資料管治和機構性措施

2.風險評估

3.技術上及操作上的保安措施

4.資料處理者的管理

5.資料保安事故發生後的補救措施

6.監察、評估及改善

7.其他考慮

下載指引

下載小冊子

網絡安全建議措施

技術上及操作上的保安措施

資料使用者應採取**足夠及有效的保安措施**，以保護其控制或所持有的個人資料和資訊及通訊系統：

網絡安全建議措施

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；
- 及時更新正在使用的系統及軟件，以**修補保安漏洞**，減少被攻擊的機會。

網絡安全建議措施

資料保安事故發生後的補救措施

- 停止並中斷連接受影響的系統
- 更改密碼或中止權限
- 更改系統配置
- 通知受影響人士並提供建議
- 通知私隱公署及其他執法或監管機構
- 修補保安漏洞
- 在可行情況下掃瞄系統
- 汲取經驗及教訓

NOTE

資料使用者亦應從資料保安事故中汲取經驗及教訓，覆檢和加強其整體資料治理和資料保安措施

其他資訊科技相關指引及報告

- 保障個人資料私隱 – 使用社交媒體及即時通訊軟件的指引
- 個人資料匿名化入門指南
- 私隱專員公署完成審查60間機構使用人工智能對個人資料私隱的影響
- 僱員使用生成式AI的指引清單
- 人工智能 (AI): 個人資料保障模範框架
- 雲端運算指引
- 《數碼時代的私隱保障：實測十個網上旅遊平台收集個人資料的情況》報告
- 《電子點餐的私隱關注》報告
- 使用AI聊天機械人「自保」十招
- 《數碼時代的私隱保障：比較十大網購平台的私隱設定》報告
- 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
- 資訊及通訊科技系統的貫徹數據保障設計指引

www.pcpd.org.hk

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

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

Thank you!

謝謝！