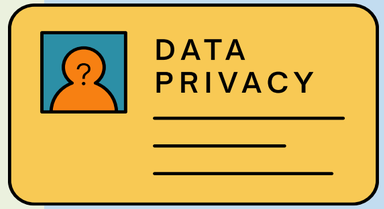
消費者委員會
CONSUMER COUNCIL

調查報告

消費者委員會
資訊系統遭勒索軟件攻擊

根據香港法例第486章《個人資料（私隱）條例》第48(2)條發表

2024年5月2日



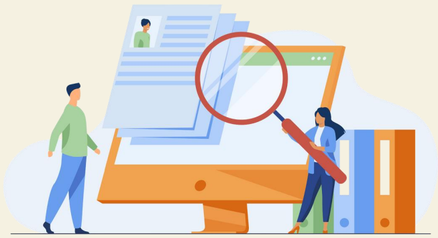
PCPD.org.hk

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

事件背景

- **2023年9月21日，消費者委員會（消委會）向公署通報資料外洩事故，表示其伺服器遭受到勒索軟件攻擊（該事件）**

公署的調查



- 在接獲上述資料外洩事故通報後，公署對消委會展開調查，以確定消委會在該事件中的作為或行為是否涉及違反《個人資料（私隱）條例》（《私隱條例》）的規定
- 專員就消委會在該事件發生時採取的保安措施共進行了**五次查訊**，並審視了消委會提供的資料，包括消委會委聘的網絡安全專家提供的調查報告，以及消委會就該事件的跟進及補救措施

事件背景

黑客組織ALPHV獲取並利用消委會一個具管理員權限的帳戶透過虛擬私有網絡進入消委會的網絡

2023年9月4日

消委會伺服器及端點裝置遭受到勒索軟件攻擊

2023年9月19-20日

消委會向公署通報該事件

2023年9月21日

受影響的個人資料

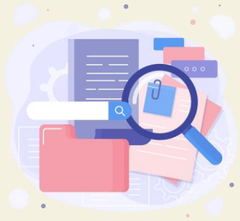
- 網絡安全專家確實該事件涉及的數據少於1.5GB，而該些數據包括黑客進入消委會後進行的活動（例如網絡掃瞄）
- 在該事件中，四個載有個人資料的檔案遭受未獲准許的查閱，**涉及超過450名人士的個人資料，包括投訴人、資訊科技服務供應商的員工、消委會的現職及已離職員工**

受影響的個人資料

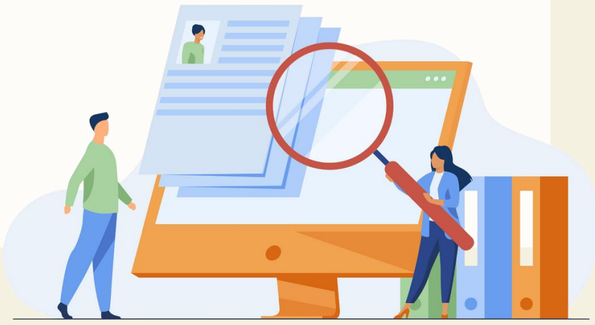
	受影響人士的類別及人數	受影響的個人資料
01	289名投訴人	姓名、手提電話號碼、住宅或通訊地址、電郵地址、收入範圍、年齡範圍及／或投訴性質及簡要（如投訴人有提供相關資料[1]）
02	26名資訊科技服務供應商員工	姓名、職銜、電郵地址、公司電話號碼及／或手提電話號碼[2]
03	138名現職及24名已離職的消委會員工[3]	姓名、所屬部門名稱、公司電話號碼及／或職銜[4]

[1]其中57名投訴人未有提供住宅地址及五名投訴人未有提供完整地址，以及14名投訴人提供非住宅地址。另外，四名投訴人未有提供電郵地址
[2]五名人士未有提供手提電話號碼
[3]該事件發生時的人數
[4]只涉及一名現職員工的職銜

調查結果



- 黑客組織取得消委會一個具有管理員權限的帳戶憑證，隨後透過虛擬私有網絡（VPN）進入消委會的網絡，並對消委會的伺服器及端點裝置進行勒索軟件攻擊
- 該事件導致消委會的**93個系統**遭到惡意加密，**11個伺服器及端點裝置**被黑客入侵



《私隱條例》的相關規定

- 消委會控制受該事件影響的人士的個人資料的收集、持有、處理及使用，因此屬《私隱條例》第2(1)條釋義下的資料使用者，須遵從《私隱條例》的規定行事，包括《私隱條例》附表1所列明的六項保障資料原則
- 根據《私隱條例》附表1保障資料第4(1)原則有關個人資料保安的規定，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

調查結果

經考慮與該事件有關的事實及在調查過程中所獲得的證據，**專員認為該事件是由以下五項缺失導致：**

1. 沒有為遠端存取資料啟用多重認證功能
2. 沒有妥善設定用作偵測及攔截網絡安全威脅的網絡安全軟件
3. 欠缺足夠保安措施禁止或防止於測試伺服器內儲存個人資料
4. 資訊保安政策有欠全面及具體
5. 保障個人資料私隱及網絡安全意識不足

調查結果

01 沒有為遠端存取資料啟用多重認證功能

2020年11月

- 消委會實施在家工作安排，**允許員工透過VPN遠端連接消委會的網絡**
- 考慮到員工對採用多重認證功能的阻力及資訊科技部人手不足以在不影響運作的情況下為所有員工安裝有關程式，**消委會未有為遠端存取資料啟用多重認證功能以核實獲授權可遠端登入消委會網絡的用戶**

2022年5月

- 消委會取消在家工作安排，但**仍允許員工在沒有多重認證功能的情況下遠端連接消委會的網絡**

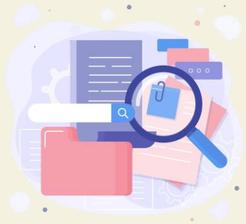
事發後暫停遠端存取資料的安排

調查結果

01 沒有為遠端存取資料啟用多重認證功能

- 在該事件中，黑客組織獲取並利用消委會一個具管理員權限的帳戶憑證進入消委會的網絡。若然消委會有為遠端存取資料啟用多重認證功能以確認該帳戶的用戶身分，這便可能阻止黑客透過該帳戶進入消委會的網絡，亦可避免隨後的勒索軟件攻擊及黑客查閱系統當中儲存的個人資料
- 消委會在該事件發生時未有啟用多重認證功能，以核實獲授權可遠端登入消委會網絡的用戶身分，是導致該事件發生的重要原因

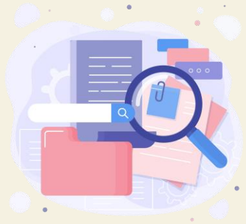
調查結果



02 沒有妥善設定用作偵測及攔截網絡安全威脅的網絡安全軟件

- 自2020年5月起，消委會使用網絡安全軟件以偵測及攔截網絡安全威脅，並向消委會發出警報
- 該事件發生後，消委會發現該網絡安全軟件在該事件中未能攔截黑客進入消委會網絡後所進行的活動，亦未有啟動該網絡安全軟件的警報功能，令該網絡安全軟件未能在偵測到網絡安全威脅後向消委會發出警報電郵。由於負責該網絡安全軟件的消委會員工及供應商員工均已離職，消委會未能確定有關原因

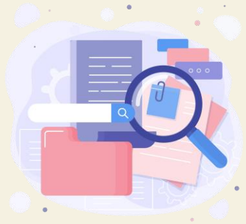
調查結果



02 沒有妥善設定用作偵測及攔截網絡安全威脅的網絡安全軟件

- 由於消委會未有妥善設定該網絡安全軟件，導致該網絡安全軟件未能發揮作用
- 倘若消委會在事發前有審視該網絡安全軟件的效能及設定，或已修正該網絡安全軟件的設定，應可增加消委會在該事件中發現黑客早期活動的機會，從而避免勒索軟件攻擊及個人資料遭受未獲准許的查閱
- 在事發後，消委會已修正該網絡安全軟件的設定，以在偵測網絡安全威脅後向消委會發送警報電郵

調查結果



03 欠缺足夠保安措施禁止或防止於測試伺服器內儲存個人資料

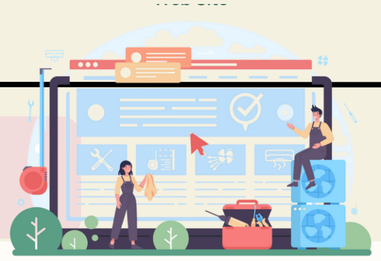
- **289**名投訴人的個人資料因**人為錯誤或疏忽**，自2023年6月起（即該事件發生前三個月）被儲存於沒有配置網絡安全軟件的一個測試伺服器內，隨後遭受黑客攻擊
- 消委會表示無意於測試伺服器內儲存個人資料，但事發時消委會**沒有任何書面政策禁止或防止員工儲存個人資料於測試伺服器內**

調查結果

03 欠缺足夠保安措施禁止或防止於測試伺服器內儲存個人資料

- 原則上，考慮到測試伺服器的保安措施一般較弱，機構不應將真實的個人資料儲存於測試伺服器內
- 若消委會在事發時已制訂政策禁止或防止於測試伺服器內儲存個人資料、明確通知員工相關政策及制訂程序定期審視測試伺服器內的資料，便可減低人為錯誤或疏忽的風險
- 消委會欠缺足夠保安措施禁止或防止於測試伺服器內儲存個人資料，導致投訴人的個人資料被儲存於沒有配置網絡安全軟件的測試伺服器內，屬其中一項缺失

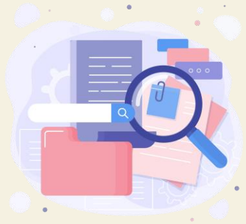
調查結果



04 資訊保安政策有欠全面及具體

- 消委會就資訊保安方面制訂的政策及指引只列出資訊科技部門日常工作的程序及訂明一般性原則，**未有提供全面及具體的網絡保安框架或資訊科技保安檢視規定及程序供員工依循**
- **資訊保安政策應訂定資訊保安管理框架及提供具體的操作程序及／或指引**，例如員工的角色及責任、進行保安審計的程序等資訊，讓員工有一個具體的網絡保安框架可依循

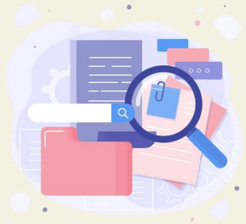
調查結果



05 保障個人資料私隱及網絡安全意識不足

- 消委會表示在該事件發生前有提供員工培訓及傳閱與網絡安全相關的資訊。然而，除了因人為錯誤或疏忽而儲存個人資料於測試伺服器外，調查亦發現一名前資訊科技部員工沒有於系統設定實施消委會訂定的複雜密碼政策，令有關政策在事發時未有被貫徹實施

調查結果



- 調查顯示消委會在該事件發生之前未有採取所有切實可行的步驟以確保涉事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，因而**違反了《私隱條例》保障資料第4(1)原則**有關個人資料保安的規定
- 專員已**向消委會送達執行通知**

向消委會發出執行通知

1. 為所有遙距存取載有個人資料的系統**實施多重身分認證**，並定期檢視遙距存取的權限

2. **聘請獨立的資訊安全專家**檢視資訊系統的保安措施，確保該些系統具備有效的偵測及保安措施

3. **定期檢視資訊系統的保安措施**，包括但不限於網絡安全軟件的設定，以確保該些系統具備有效的偵測及保安措施

4. **制訂清晰及全面的政策及程序**，以禁止或防止於測試伺服器內儲存個人資料

向消委會發出執行通知

5.制訂清晰及全面的資訊系統保安政策及程序，涵蓋防範、偵測及應對網絡攻擊的各種管控措施、進行風險評估及保安審計的要求

6.制訂並實施有效措施以確保員工遵循上述第(4)及(5)項的政策及程序

7.加強數據安全及資料保護的培訓，每年至少為全體員工舉辦一次講座／研討會／工作坊，並建立評估機制，確保員工準確理解相關課程內容

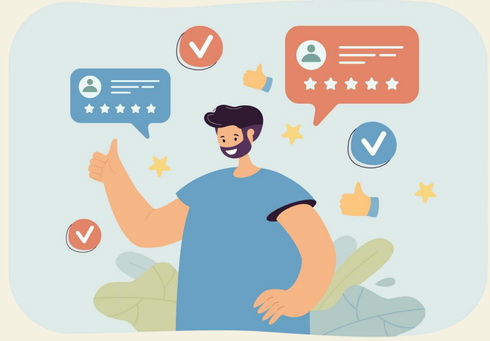
8. 由執行通知的日期起計兩個月內向專員提供文件，證明已完成上述第(1)至(7)項指示

建議

01 對遙距登入資訊及通訊系統**使用多重身分驗證**，以減低資訊系統被攻擊的風險

02 **設立穩健的網絡保安框架**，在防範、偵測及應對網絡攻擊方面投放足夠資源及制訂有效的策略及措施，以減低被攻擊的可能性及資料外洩風險

03 定期對資訊系統**進行風險評估及保安審計**



04 **建立重視數據安全的企業文化**

05 **建立有效的培訓計劃**，加強員工就數據安全及個人資料私隱方面的意識及能力

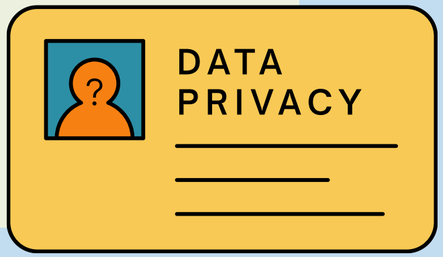
消費者委員會
CONSUMER COUNCIL

Investigation Report

Ransomware Attack on the Information Systems of the Consumer Council

Published under Section 48(2) of the Personal Data (Privacy) Ordinance (Cap 486)

2 May 2024



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

Background

- The investigation arose from a data breach notification lodged by the Consumer Council (the Council) on 21 September 2023, reporting that its servers had been attacked by ransomware (the Incident)
- Upon receipt of the data breach notification from the Council, the Privacy Commissioner for Personal Data (the Commissioner) commenced an investigation against the Council regarding the Incident to assess whether the Council's acts or practices relating to the Incident had contravened the requirements of the Personal Data (Privacy) Ordinance (PDPO)

Background

- During the investigation, the Commissioner:-
  - ❑Conducted five rounds of enquiries regarding the security measures adopted by the Council at the time of the Incident
  - ❑Examined various information provided by the Council relating to the Incident, including an investigation report provided by an independent cybersecurity expert (Security Expert) engaged by the Council
  - ❑Considered the follow-up and remedial measures taken by the Council in the wake of the Incident

Personal Data and Data Subjects Affected

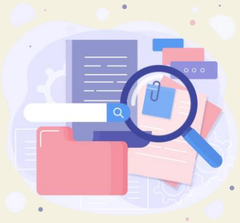
- The volume of data involved in the Incident was less than 1.5GB. The figure included traffic data generated by the hacker's activities (e.g. network scanning)
- The Incident resulted in unauthorised access to four files containing the personal data of more than 450 individuals, including complainants, personnel of information technology service vendors, and current and former staff members of the Council

Personal Data and Data Subjects Affected

	Types and Numbers of Affected Data Subjects	Personal Data Affected
01	289 Complainants	Names, mobile phone numbers, residential / communication addresses, email addresses, income ranges and age ranges, brief nature and/or information about the complaints (if provided by the complainants[1])
02	26 Personnel of Information Technology Service Vendors	Names, titles, email addresses, office telephone numbers and/or mobile phone numbers[2]
03	138 Current and 24 Former Staff Members[3] of the Council	Names, work divisions, office telephone numbers and/or title[4]

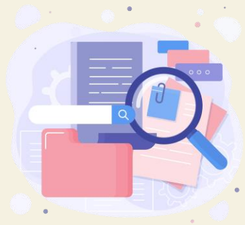
[1] 57 complainants did not provide residential address and five provided incomplete addresses. 14 complainants provided non-residential addresses. Four complainants did not provide any email address
[2] Five individuals did not provide mobile phone numbers
[3] Figures as at the time of the Incident
[4] Only involved one current staff member's title

Findings of Investigation



- On 4 September 2023, a hacker group identified as ALPHV had obtained the credentials of a user account with administrative privileges and gained access to the Council's network through a Virtual Private Network
- The hacker deployed ransomware in the servers and endpoints of the Council between 19 and 20 September 2023. **93 systems of the Council were maliciously encrypted and 11 servers and workstations were accessed by the hacker**

Findings of Investigation



The Commissioner considers that the Incident was caused by the following deficiencies of the Council:

1. **Failure to enable multi-factor authentication for remote access to data, thereby allowing the hacker to gain access to the Council's network through the compromised account credentials, conduct ransomware attack and access the personal data held by the Council**

2. **Failure to properly configure the cybersecurity solutions adopted to detect and block cybersecurity threats, resulting in the failure of the cybersecurity solutions to send email alerts to the Council when cybersecurity threats were detected**

3. **Lack of sufficient safeguard to prohibit or prevent the storage of personal data on testing servers, which led to the personal data of 289 complainants held by the Council being stored in a testing server that was not protected by the cybersecurity solutions because of human error or oversight, and in turn, exposed to hacking attack**

Findings of Investigation

The Commissioner considers that the Incident was caused by the following deficiencies of the Council:

4. Lack of specificity and comprehensiveness in the policies on information security, which did not provide a concrete cybersecurity framework or IT security review requirements and procedures for its staff members to follow

5. Inadequate awareness of information security and data protection: Apart from the storage of personal data on the testing server owing to human error or oversight, the investigation also revealed that a former IT staff member had not enforced the complex password policy of the Council in the system settings at the time of the Incident, rendering its password policy ineffective

Findings of Investigation

- The Council had not taken all practicable steps to ensure that the personal data involved was protected against unauthorised or accidental access, processing, erasure, loss or use, thereby **contravening Data Protection Principle 4(1) of the PDPO concerning the security of personal data**
- The Commissioner has served an **enforcement notice** on the Council, directing it to remedy the contravention and prevent similar recurrence of the contravention

Enforcement Notice Served on the Council

1. **Implement multi-factor authentication of all remote users** accessing the Consumer Council's information systems which contain personal data, and conduct regular reviews of remote access privileges

2. **Engage an independent information security expert to review the security measures of the Consumer Council's information systems** to ensure that the information systems have effective detection and security measures in place

3. **Regularly review the security measures of the Consumer Council's information systems**, including but not limited to the configuration of cybersecurity solutions, to ensure that the information systems have effective detection and security measures in place

4. Devise clear and comprehensive policies and procedures to **prohibit or prevent the storage of personal data on testing server(s)**

Enforcement Notice Served on the Council

5. **Devise clear and comprehensive information security policies and procedures** to cover control measures for preventing, detecting and responding to cyberattacks, as well as the requirements on conducting risks assessments and security audits

6. **Devise and implement effective measures to ensure staff compliance** with the policies and procedures stated in items (4) and (5) above

7. **Strengthen training on data security and data protection** by organising talks/seminars/workshops for all staff members at least once a year, and establish an assessment mechanism to ensure accurate understanding of the relevant course content

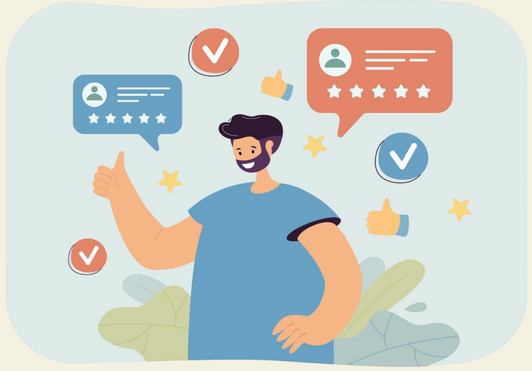
8. Provide documentary proof to the Commissioner **within two months** from the date of this Enforcement Notice, showing the completion of items (1) to (7) above

Recommendations

01 **Adopt multi-factor authentication** for remote access to information and communications systems to minimise the risk of attacks targeting information systems

02 **Establish a robust cybersecurity framework**, allocate sufficient resources and formulate effective strategies and measures to prevent, detect and respond to cyberattacks, thereby reducing the possibility of cyberattacks and the risk of data leakage

03 Conduct regular risk assessments and security audits of information systems



04 Establish a corporate culture that values data security

05 **Devise effective training plans** to enhance staff awareness and competence in data security and personal data protection

END