調查報告

根據香港法例第 486 章《個人資料(私隱)條例》
第 48(2) 條發表

日經中國（香港）有限公司

的電郵系統遭黑客入侵

報告編號：R22 - 7840
發表日期：2022 年 2 月 17 日

調查報告：日經中國（香港）有限公司的電郵系統遭黑客入侵

香港法例第 486 章《個人資料（私隱）條例》（《私隱條例》）第 48(2)條訂明，「[個人資料私隱]*專員在完成一項調查後，如認為如此行事是符合公眾利益的，可－*

(a)　發表列明以下事項的報告－

(i)　該項調查的結果；

(ii)　由該項調查引致的、專員認為是適合作出的關乎促進有關資料使用者所屬的某類別的資料使用者遵守本條例條文（尤其是各保障資料原則）的任何建議；及

(iii)　由該項調查引致的、專員認為適合作出的任何其他評論；及

(b)　以他認為合適的方式發表該報告。」

現根據《私隱條例》第 48(2)條履行所賦予的權力，發表本調查報告。

鍾麗玲
個人資料私隱專員
2022 年 2 月 17 日

目錄

調查報告

根據香港法例第 486 章《個人資料（私隱）條例》第 48(2) 條發表

日經中國（香港）有限公司
的電郵系統遭黑客入侵

摘要

背景

1. 2021 年 3 月 17 日，個人資料私隱專員公署（私隱公署）收到日經中國（香港）有限公司（日經）的資料外洩事故通報，指其六個員工的電郵帳戶曾遭黑客入侵，導致於 2020 年 10 月至 2021 年 2 月期間共超過 1,600 名日經的客戶發送至該些電郵帳戶的電郵被轉發至兩個不明的電郵地址（該事件）。經電郵外洩的客戶個人資料包括客戶的姓名、電郵地址、公司名稱、電話號碼及信用卡資料。

2. 在接獲該資料外洩事故通報後，私隱公署隨即對日經展開循規審查，以取得更多有關該事件的資料。在收到日經所提供的進一步資料後，個人資料私隱專員（專員）相信日經在該事件中的作為或行為可能涉及違反香港法例第 486 章《個人資料（私隱）條例》（《私隱條例》）的規定，遂於 2021 年 5 月根據《私隱條例》第 38(b)(ii)條就該事件對日經展開調查。

調查

3. 專員在進行調查的過程中，審視了日經提供與該事件有關的資訊，包括資料外洩事故通報及日本經濟新聞社於其網站作出的公告，就日經資訊系統及電郵系統的保安措施進行了七次的查訊，並審視了日經所委任的獨立網絡安全顧問公司提供的調查報告。此外，專員亦考慮了日經在該事件發生後的跟進及補救工作。

調查結果及違例事項

資料外洩事故

4. 專員得悉黑客獲得了一個日經為員工與客戶溝通而設立的電郵帳戶的密碼，繼而為該電郵帳戶和另外五個使用相同密碼的電郵帳戶設置轉發功能，將所有收到的電郵自動轉發至該兩個不明電郵地址。

5. 在有關電郵帳戶被黑客入侵時，1,644 名客戶於 2020 年 10 月至 2021 年 2 月期間向日經發送的電郵被查閱並轉發至看來是由黑客控制的兩個不明電郵地址。經電郵外洩的客戶個人資料包括客戶的姓名、電郵地址、公司名稱、電話號碼及信用卡資料。

6. 由於日經控制受該事件影響的個人資料的收集、持有、處理或使用，日經屬《私隱條例》下的資料使用者，須依循《私隱條例》的規定行事，包括《私隱條例》附表一所列明的六項保障資料原則。

日經違反保障資料第 4(1)原則

7. 根據保障資料第 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。

8. 然而，根據調查所獲得的證據，專員發現日經的電郵系統在所有關鍵時間在保安方面明顯地存在以下四項不足。

(1) 薄弱的密碼管理

被入侵的六個電郵帳戶使用相同密碼，而有關密碼是建立該些電郵帳戶時由電郵服務供應商提供的預設密碼，密碼只是由一組短長度的數字組成，本質上屬極低強度密碼。專員亦發現由於日經的員工未有完全知悉母公司的密碼管理政策導致他們在這方面的資訊保安認知有所不足。這使到有關的預設密碼未被更改。

(2) 保留已過時的電郵帳戶

在該事件發生之時，日經的電郵系統中有 24 個電郵帳戶屬已離職員工的電郵帳戶，而這些電郵帳戶已不被使用。被入侵的六個電郵帳戶的其中一個屬於一名於該事件發生時已退休的員工。日經沒有對其電郵系統的不活躍或休眠帳戶進行任何常規檢視或審核。

(3) 電郵系統欠缺針對遠端存取的保安措施

日經的電郵系統包括允許遠端存取的網頁郵件服務，但沒有保安監察及警報功能以提示系統管理員任何來自異常或不明的 IP 位址查閱或登錄系統。日經沒有對網頁郵件服務進行內部常規審核，或對資訊保安的措施進行外部審核。

(4) 欠缺針對資訊系統的保安措施

日經缺乏處理敏感個人資料（包括信用卡資料）的政策、程序和措施，亦缺乏管控措施以確保員工透過加密的渠道查閱其電郵帳戶，以防止密碼在不安全的網絡上被截取。

9. 該事件揭示了日經沒有採取適當的保安政策、程序及措施以防範其電郵系統遭到網絡攻擊，導致黑客入侵其電郵系統令客戶的個人資料遭未經授權的查閱、處理或使用。**在本案中，專員認為日經未有採取所有切實可行的步驟保障其持有的客戶個人資料不受未獲准許的或意外的查閱、處理、刪除或使用所影響，因而違反了保障資料第 4(1)原則有關個人資料保安的規定。**

執法行動

10. 專員已向日經送達執行通知，指示日經採取以下步驟以糾正以及防止有關違規情況再發生：

(1) 修訂資訊保安政策，加入並詳細說明強密碼管理政策、定期刪除已過期或不再使用的電郵帳戶機制，及訂立系統以定時監察及審核（包括內部審核）電郵帳戶的使用情況。

(2) 制訂有效措施以確保員工依循已修訂的資訊保安政策。

(3) 聘請獨立的資料保安專家對日經的系統保安，包括電郵系統進行定期檢視及審核。

(4) 為員工制定最新的資訊保安培訓，並妥善記錄培訓進度，以及對培訓的參與及有效程度作出評估。

(5) 由執行通知的日期起計兩個月內提供文件，證明已完成上述第 (1)至 (4)項。

建議

11. 專員希望藉此報告，提醒處理包含客戶個人資料的電郵的機構需加強警惕，以防止網絡攻擊影響其電郵系統。機構應制定適當的系統安全政策、措施和程序，並涵蓋以下領域。

(1) **設立個人資料私隱管理系統：**機構應建立及維持一套遵從《私隱條例》規定的系統，循規地使用個人資料。個人資料私隱管理系統有助機構管理由收集至銷毀個人資料的整個生命週期，令機構可迅速應對任何資料外洩事故，並確保遵從《私隱條例》。設立個人資料私隱管理系統可幫助機構贏得客戶及其他持份者的信任。

(2) **委任保障資料主任：**機構應委任員工負責監察《私隱條例》的遵從並向高級管理層匯報。保障資料主任的職責是把客戶關注的保障資料問題和涉及客戶個人資料事故的經驗納入機構的資料保障政策中，並安排提供相關培訓予員工以提升他們對個人資料保障的認知及知識。

(3) **電郵通訊政策：**機構應該對其持有的個人資料的種類以及允許員工透過電郵傳送資料的情況進行分類。機構亦應考慮限制敏感個人資料只能由獲授權人員發送，並實施程序以確保只有獲授權人員才能保管及存取包含敏感個人資料的電郵。

(4) **保安措施：**如果機構允許通過電郵發送敏感的個人資料，可行的方法是在發送前對資料進行加密，以防止個人資料遭未經授權的攔截或存取。如收到載有未加密的敏感個人資料的電郵，應確保安全儲存資料。另外，當機構選擇電郵服務供應商時應審視相關供應商所採取的保安措施，當中應包括有關軟件的系統保安，以及是否提供審計紀錄等。

(5) **工作場所的私隱友善文化：**員工應了解尊重及保護個人資料私隱，以及遵守《私隱條例》規定的重要性。他們應該在資料保障程序方面獲得足夠的培訓，並在處理含個人資料的電郵時格外留神。

I. 背景

1. 2021 年 3 月 17 日，個人資料私隱專員公署（私隱公署）收到日經中國（香港）有限公司（日經）的資料外洩事故通報，指其六個員工的電郵帳戶遭黑客入侵，導致於 2020 年 10 月至 2021 年 2 月期間共超過 1,600 名日經的客戶發送至該些電郵帳戶的電郵被轉發至兩個不明的電郵地址（該事件）。經電郵外洩的客戶個人資料包括客戶的姓名、電郵地址、公司名稱、電話號碼及信用卡資料。

2. 同日，日經的母公司日本經濟新聞社就該事件發佈一則標題為「*Unauthorized access to email account of Nikkei China (Hong Kong) Limited*」的公告[1]（該公告）。

3. 在接獲該資料外洩事故通報後，私隱公署隨即對日經展開循規審查，以取得更多有關該事件的資料[2]。在收到日經所提供的進一步資料後，個人資料私隱專員（專員）相信日經在該事件中的作為或行為可能涉及違反香港法例第 486 章《個人資料（私隱）條例》（《私隱條例》）的規定，遂於 2021 年 5 月根據《私隱條例》第 38(b)(ii)條就該事件對日經展開調查。

---

1 https://www.nikkei.co.jp/nikkeiinfo/en/news/announcements/759.html

2 見 2021 年 3 月 18 日標題為「私隱專員就日經電郵系統遭入侵事件展開循規審查」的新聞稿 (https://www.pcpd.org.hk/tc_chi/news_events/media_statements/press_20210318.html)。

II. 法定權力

4. 專員的權力是根據《私隱條例》所賦予的。根據《私隱條例》第8(1)條，專員須就遵守《私隱條例》條文作出監察及監管，以及促進對《私隱條例》的條文的認識及理解以及遵守。

5. 《私隱條例》第 38 條授權專員在下述情況下可進行調查：

(i) 當專員收到由受影響的資料當事人或其代表作出的投訴，除《私隱條例》第 39 條另有規定外，專員須根據第 38(a)及(i)條對有關的資料使用者進行調查，以確定在有關的投訴中指明的作為或行為是否屬違反《私隱條例》下的規定；或

(ii) 當專員有合理理由相信有資料使用者已經或正在作出或從事關乎個人資料的作為或行為，而有關作為或行為可能違反《私隱條例》下的規定，專員可根據第 38(b)及(ii)條對資料使用者進行調查，以確定有關行為或作為是否屬違反《私隱條例》下的規定。

6. 專員在展開調查後，可根據《私隱條例》第 43(1)(a)條，為調查的目的而自她認為合適的人處獲提供她認為合適的資訊、文件或物品，以及作出她認為合適的查訊。

7. 《私隱條例》第 48(2)(a)條訂明，專員在完成調查後，如認為如此行事是符合公眾利益的，可發表報告列明該項調查的結果及由該項調查引致的、專員認為適合作出的任何建議或其他評論。

8. 根據《私隱條例》第 50(1)條，如專員在完成一項調查後，認為有關的資料使用者正在或已經違反《私隱條例》的規定，專員可向該資料使用者送達書面通知，指示該資料使用者糾正該項違反，以及（如適當的話）防止該項違反再發生。

9. 根據《私隱條例》第 50A 條，資料使用者違反執行通知，即屬犯罪，一經首次定罪，最高可被判處第五級罰款（即港幣 50,000 元）及監禁兩年。

III. 該事件的相關事實及情況

10. 專員在進行調查的過程中，審視了日經提供與該事件有關的資訊，包括資料外洩事故通報及該公告，就日經資訊系統及電郵系統的保安措施進行了七次的查訊，並審視了日經所委任的獨立網絡安全顧問公司（該網絡安全顧問公司）提供的調查報告。此外，專員亦考慮了日經在該事件發生後的跟進及補救工作。

公司背景

11. 日經是日本經濟新聞社的香港子公司，透過印刷及網上形式提供新聞和分析資訊。香港的企業及個人客戶可以訂購日經的服務，利用網頁、流動裝置或每日及每週印刷版閱讀日經提供的新聞及分析資訊。

日經的資訊保安政策

12. 日經在該事件發生之時訂有一套「*資訊管理規定*」（Information Management Regulations），就其擁有的資料釐定了整體的保安管理框架。日經把上述規定存放於一個所有員工都可查閱的共享文件夾中，並口頭要求員工仔細閱讀當中的內容。

13. 日本經濟新聞社於 2018 年 5 月發出了一份「*保安管理措施要求列表*」（Table of Requirements for Security Management Measures）（母公司的保安政策），對包括日經在內的整個集團的公司所需採取的資訊保安措施提供了實務指引，包括密碼政策，當中訂明了密碼的最低長度及所需的複雜程度。

日經的電郵系統

14. 日經自 2011 年起使用由同一間服務供應商（該服務供應商）提供的電郵系統（該電郵系統）。該電郵系統包括涉及該事件的網頁郵件服務[3]（該網頁郵件服務）。

15. 日經表示在該事件之前他們未有就該電郵系統進行定期保安檢視。

16. 根據日經提供的資料，在該事件發生之時共設有 41 個電郵帳戶，當中 24 個屬已離職員工的電郵帳戶，已不再被員工使用。

該事件的曝光

17. 2021 年 3 月 1 日，日經的一名員工接獲一封電郵傳遞錯誤的通知，指未能成功發送一封電郵至一個不明的電郵地址。由於日經認為情況可疑，遂作出檢查並發現大量收到的電郵被自動轉發至不明的電郵帳戶。日經隨即委託該網絡安全顧問公司進行徹底調查，發現一個未經授權的外部帳戶擁有日經六個電郵帳戶（該六個電郵帳戶）的控制權限。該未經授權的外部帳戶把該六個電郵帳戶收到的電郵自動轉發至兩個不明的電郵地址（該兩個不明電郵地址）。

18. 調查亦發現上述未經授權的轉發電郵活動自 2020 年 10 月已在進行。在 2020 年 10 月至 2021 年 2 月期間，約有 16,860 封電郵被轉發至該兩個不明電郵地址。

19. 日經表示其中一個受影響的電郵帳戶屬於一名當時已退休的員工，而其餘五個電郵帳戶屬於不同職位的員工，他們負責解答查詢，與客戶、代理商及受訪者進行溝通等工作。

[3] 該網頁郵件服務是由該服務供應商提供的電子郵件代管服務，是一個建基於第三方產品並透過 IMAP、POP3、ActiveSync 的規約提供多用戶電子郵件代管服務。 該網頁郵件服務允許電郵帳戶擁有人設定電郵轉寄功能。

受影響的個人資料

20. 日經表示 1,644 名客戶的個人資料可能在該事件中遭外洩，當中涉及香港及海外的企業及個人客戶：

	受該事件影響人數
香港客戶	650
海外客戶	994

21. 日經表示受影響的企業客戶的個人資料包括姓名、職稱、電郵地址、電話號碼及其所屬的公司名稱；而受影響的個人客戶的個人資料包括姓名、電話號碼及電郵地址。該事件亦影響 18 名個人客戶及四名企業客戶的信用卡資料（包括信用卡號碼、卡主姓名及到期日）。

22. 日經表示儘管多次向該服務供應商提出要求，但由於該服務供應商沒有充分地保留超過兩個月的日誌紀錄，日經因而無法追踪黑客首次入侵該六個電郵帳戶的確切日期。

該網絡安全顧問公司的調查結果

23. 該網絡安全顧問公司表示，由於該電郵系統缺乏由該服務供應商保存的日誌紀錄，導致未能確定黑客是如何入侵該六個電郵帳戶。儘管如此，該網絡安全顧問公司確認了以下事實。

(i) 所有該六個電郵帳戶收到的電郵自 2020 年 10 月 29 日起已被自動轉發至該兩個不明電郵地址中的其中一個電郵地址。黑客因而在 2020 年 10 月至 2021 年 2 月期間取得所有傳送至該六個電郵帳戶的電郵的複本。

(ii) 該網頁郵件服務是設定或更改轉發的電郵地址的唯一途徑。

(iii) 在該服務供應商提供的該網頁郵件服務建基的軟體版本中，並不存在已被知悉的相關漏洞。因此，可以排除黑客是經軟體版本的漏洞而對電郵帳戶進行存取的可能性。

(iv) 該網頁郵件服務不支援多重認證功能。

(v) 日經沒有定期檢視該電郵系統的系統配置。

(vi) 該六個電郵帳戶在 2021 年 3 月之前一直沿用同一組密碼。該組密碼是該服務供應商在建立電郵帳戶時預設的，只包含一組短的數字。使用其他密碼的日經電郵帳戶在該事件中未有受到影響。

(vii) 日經既無規定員工更改電郵帳戶的預設密碼，亦無要求他們定期變更電郵帳戶的密碼。

(viii) 該網絡安全顧問公司在該事件後進行的保安檢視中識辨出該服務供應商提供的該網頁郵件服務及日經的資訊系統中的一些缺失[4]，惟沒有跡象顯示該些缺失直接引發該事件。

(ix) 日經在該事件之前一直透過電郵接收未經加密的信用卡資料，且在把這些資料提交至銀行進行交易之後沒有把資料從電郵帳戶的收件匣中刪除。

[4] 為保障可能被用作損害日經資訊系統安全的敏感資料，有關詳情被略去。

24. 該網絡安全顧問公司提供的調查報告確認黑客取得該六個電郵帳戶中其中一個帳戶的密碼。在發現該組密碼同時可對另外五個電郵帳戶進行存取後，黑客於是對該些帳戶展開攻擊。

25. 雖然沒有足夠證據顯示黑客是如何取得密碼，但該網絡安全顧問公司羅列了幾種可能與該事件有關的攻擊方法：

(i) 由於該六個電郵帳戶沿用的預設密碼強度欠奉，密碼可以輕易透過暴力攻擊[5]取得；

(ii) 密碼可透過仿冒詐騙[6]的方法取得；及

(iii) 當日經的員工在不安全的無線網絡使用他們的移動設備存取電郵帳戶時，密碼可透過網路監聽[7]取得。

日經採取的跟進工作及補救措施

26. 在調查的過程中，日經發現該服務供應商提供的該網頁郵件服務及日經的資訊系統在資料保安方面存在以下不足之處：

(i) 接收沒被加密的信用卡資料；

(ii) 該服務供應商提供的該網頁郵件服務欠缺多重認證功能；

(iii) 欠缺強密碼保安措施；

(iv) 該服務供應商為不同的電郵帳戶設定相同的預設密碼；

---

5 暴力攻擊是嘗試所有可能性以破解加密或認證系統的技術。

6 仿冒詐騙是一種社交工程攻擊，仿冒詐騙者通常使用虛假網站、電郵、即時通訊或短訊服務等形式進行攻擊，這些訊息中通常包含被惡意軟件感染的附件或惡意網站的超連結，目的是竊取用戶的敏感資料（例如登入憑證、銀行帳戶或信用卡資料等）和／或入侵用戶的電腦裝置。

7 是一種監視網路狀態、數據流程以及網路上信息傳輸的管理工具。

(v) 該服務供應商設定的預設密碼由一組短長度的數字組成，屬低強度密碼；及

(vi) 該服務供應商沒有充分地保留超過兩個月的日誌紀錄。

27. 該網絡安全顧問公司亦總結地指出，該服務供應商提供的服務未達企業級標準以供企業客戶使用，此等保安水平使日經的資訊系統暴露於黑客的惡意攻擊中。日經在發現該事件後，隨即委託該網絡安全顧問公司進行徹底調查，以確認起因並部署補救措施。

28. 在 2021 年 3 月 1 日，即發現該事件當日，日經已更改該六個電郵帳戶的密碼，並停止該些帳戶的轉發功能以控制該事件衍生的損害。翌日，日經亦重設了所有其他電郵帳戶的密碼。

29. 日本經濟新聞社於 2021 年 3 月 17 日在其網站[8]發布該事件。日經向所有受影響客戶發出電郵通知，亦向受該事件影響的信用卡發卡機構通報事件。

30. 在該事件後，日經轉用由一個雲端電郵服務供應商提供的電郵系統，該系統設有強密碼保安要求並提供多重認證功能。

31. 日經亦停止透過電郵接收信用卡資料的做法，並刪除了所有載有信用卡資料的電郵訊息。

32. 日經對「*資訊管理規定*」進行了修訂並加入多項要求，包括加強監察機制及密碼要求，及收緊電郵帳戶使用政策（包括只可保留正在使用的電郵帳戶）。日經向所有員工解釋經更新的規定，並要求他們簽署確認文件以表示明白有關更新。

8 見註解 1

33. 除了為香港員工提供定期的內部培訓，日經亦進一步為其員工舉辦由外部專業人員主理的資訊安全培訓課程。這些培訓課程將每年舉行一次。

34. 日經對其資訊保安系統進行了各種提升[9]，並承諾進行年度檢視，以確保其資訊安全政策和措施能夠符合市場的最新技術發展。可在本報告披露的例子包括：

(i) 東京總部的安全中心建立了 24 小時的監察系統，以監察及辨識任何涉及日經資訊網絡的可疑活動；

(ii) 建立一套系統讓日經員工能與東京總部的技術團隊密切溝通，就技術問題尋求建議；

(iii) 該網絡安全顧問公司就有關系統升級的事宜提出多項建議，以加強日經的網絡安全，而日經已作出相應的跟進。該網絡安全顧問公司在其最終報告中確認該事件所產生的損害已得到有效控制。

[9] 為保障可能被用作損害日經資訊系統安全的敏感資料，有關詳情被略去。

IV. 有關個人資料保安的法律規定

資料使用者

35. 《私隱條例》，包括附表一的保障資料原則，旨在規管資料使用者的行為及作為。根據《私隱條例》第 2(1)條，就個人資料而言，資料使用者指「*獨自或聯同其他人或與其他人共同控制該資料的收集、持有、處理或使用的人*」。

個人資料

36. 《私隱條例》涵蓋的資料使用者在處理「個人資料」時須遵守保障資料原則，而根據《私隱條例》第 2(1)條，「個人資料」是「*指符合以下說明的任何資料—*

(a) 直接或間接與一名在世的個人有關的；
(b) 從該資料直接或間接地確定有關的個人的身分是切實可行的；及
(c) 該資料的存在形式令予以查閱及處理均是切實可行的。」

資料保安

37. 保障資料第 4(1)原則 — 資料保安原則訂明：

「 *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（包括採用不能切實可行地予以查閱或處理的形式的資料）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，尤其須考慮—*
(a) 該資料的種類及如該等事情發生便能做成的損害；
(b) 儲存該資料的地點；

(c) *儲存該資料的設備所包含（不論是藉自動化方法或其他方法）的保安措施；*

(d) *為確保能查閱該資料的人的良好操守、審慎態度及辦事能力而採取的措施；及*

(e) *為確保在保安良好的情況下傳送該資料而採取的措施。*」

38. 根據《私隱條例》第 2(1)條，「*切實可行*」指「*合理地切實可行*」。

V. 調查結果及違例事項

39. 根據保障資料第 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。在本個案中，專員已考慮：(i) 該事件是否屬資料外洩事故；(ii) 誰是須為該資料外洩事故負責的資料使用者；及(iii) 涉事的資料使用者是否已按保障資料第 4(1)原則的規定採取切實可行的步驟保障其持有的個人資料。以下是專員的調查結果。

該事件的性質

40. 資料外洩事故一般指資料使用者持有的個人資料懷疑或已遭外洩，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，從而違反保障資料第 4(1)原則的規定。

41. 基於日經在資料外洩事故通報中提供的資訊，以及日經在調查過程中提供的答覆，專員認為該事件屬資料外洩事故，當中黑客獲得了一個日經為員工與客戶溝通而設立的電郵帳戶的密碼，繼而為該電郵帳戶和另外五個使用相同密碼的電郵帳戶（即該六個電郵帳戶）設置轉發功能，將所有收到的電郵自動轉發至該兩個不明電郵地址。

42. 在該六個電郵帳戶被黑客入侵時，1,644 名客戶於 2020 年 10 月至 2021 年 2 月期間向日經發送的電郵被查閱並轉發至看來是由黑客控制的該兩個不明電郵地址。經電郵外洩的客戶個人資料包括客戶的姓名、電郵地址、公司名稱、電話號碼及信用卡資料。

43. 日經注意到該電郵系統遭未獲授權的查閱是當他們一名員工於 2021 年 3 月 1 日接獲一則電郵傳遞錯誤的通知，指一封電郵未能成功發送至一不明電郵地址。日經認為情況異常及可疑，遂檢查該電郵系

統並確認發生了該事件。日經隨即委託該網絡安全顧問公司進行調查，並其後於 2021 年 3 月 17 日將該事件通知專員。

須為該資料外洩事故負責的資料使用者

44. 日經是日本經濟新聞社的子公司，透過印刷及網上形式提供新聞和分析資訊。香港的企業及個人客戶可以訂購日經的服務，利用網頁、流動裝置或每週印刷版閱讀日經提供的新聞及分析資訊。由於日經控制受該事件影響的個人資料的收集、持有、處理或使用，日經屬《私隱條例》第 2(1)條釋義下的資料使用者，須依循《私隱條例》的規定行事，包括《私隱條例》附表一所列明的六項保障資料原則。

資料保安的不足

45. 黑客將 2020 年 10 月至 2021 年 2 月期間傳送至該六個電郵帳戶的所有電郵轉發至該兩個不明電郵地址，從而取得了這些電郵的複本。在本個案中沒有爭議的是，載有日經客戶個人資料的該電郵系統曾遭到未獲授權的查閱。

46. 該事件的主因是黑客取得了該六個電郵帳戶的預設密碼，因此能對該電郵系統進行未獲授權的查閱。專員認為有必要審視日經就該電郵系統採取的保安政策和措施。

47. 保障資料第 4(1)原則訂明，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，尤其須考慮－

(a) 該資料的種類及如該等事情發生便能做成的損害；
(b) 儲存該資料的地點；

(c) 儲存該資料的設備所包含（不論是藉自動化方法或其他方法）的保安措施；

(d) 為確保能查閱該資料的人的良好操守、審慎態度及辦事能力而採取的措施；及

(e) 為確保在保安良好的情況下傳送該資料而採取的措施。

48. 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，專員認為日經在該事件所涉及的所有期間未有發現並糾正以下四項與該電郵系統保安方面的不足，從而導致黑客利用有關漏洞入侵並查閱該電郵系統。

(1) *<u>薄弱的密碼管理</u>*

49. 根據日經提供的資料，包括該網絡安全顧問公司提供的調查報告，專員相信是以下事項導致發生了該事件：

(i) 該六個電郵帳戶同時使用一組由該服務供應商設定的密碼。具體來說，日經的員工不知道彼此密碼，他們在沒有意識到這情況下使用相同的密碼；及

(ii) 有關密碼是建立該六個電郵帳戶時由該服務供應商提供的預設密碼，密碼只是由一組短長度的數字組成。

50. 專員亦注意到使用其他密碼的日經電郵帳戶在該事件中並沒有受到影響。在這情況下，專員相信黑客是取得了有關預設密碼從而對該電郵系統作出未獲授權的查閱。

51. 在考慮日經在該事件發生時是否已採取所有切實可行的步驟以建立並維持一套有效的密碼管理制度，專員考慮了以下因素：

(i) 日經是否制定了任何密碼管理政策，以及有關的預設密碼是否符合有關政策的要求；及

(ii) 有關的密碼管理政策及／或做法是否符合普遍採用的標準。

52. 除了母公司的保安政策列明了密碼所需的長度和複雜性外，日經本身並沒有制定任何政策要求員工必須在開始使用電郵帳戶前更改由該服務供應商提供的預設密碼，亦沒有要求員工定期更改密碼。

53. 日經表示「*由於行政疏忽*，[該六個電郵帳戶]*沒有完全依從*[母公司的保安管理措施要求列表]……」（譯）。日經向專員表示他們缺乏強密碼安全措施。

54. 專員亦發現：

(i) 該六個電郵帳戶的預設密碼自電郵帳戶設立以來從未被更改過；

(ii) 由該服務供應商設定的預設密碼長度短並欠缺複雜性，本質上屬極低強度密碼，這並不符合網絡安全的基本要求，而該服務供應商為每一個電郵帳戶設定相同的預設密碼，令電郵帳戶欠缺獨有的密碼；及

(iii) 日經的員工未有完全知悉母公司的密碼管理政策導致他們在這方面的資訊保安認知有所不足。這使到有關的預設密碼未被更改。

(2) *<u>保留已過時的電郵帳戶</u>*

55. 根據日經提供的資料，在該事件發生之時該電郵系統中有 24 個電郵帳戶屬已離職員工的電郵帳戶。日經向專員確認這些電郵帳戶已不被使用。

56. 專員得悉該六個電郵帳戶的其中一個屬於一名於該事件發生時已退休的員工。專員亦注意到日經在該事件發生之前沒有對該電郵系統的不活躍或休眠帳戶進行任何常規檢視或審核。

57. 專員認為，日經應時刻警惕該電郵系統可能遭受網絡攻擊的風險，並需要維持適當的系統保安。定期檢視資訊系統的保安（包括該電郵系統）是一項基本而必須的網絡安全措施，並且應在有關系統啟動後立刻安排進行。然而，日經於關鍵時間在此事上明顯沒有進行足夠的盡職審查。

58. 專員認為，日經沒有刪除過時的電郵帳戶為自身帶來不必要的風險，並向黑客提供了機會透過該六個電郵帳戶對該電郵系統進行未獲授權的查閱，因而違反保障資料第 4(1)原則的規定。

59. 若然日經當初採取了既定政策及程序適時刪除離職員工的電郵帳戶，即使未能避免發生該事件，但本應可減輕該事件的影響及嚴重性。

(3) *該電郵系統欠缺針對遠端存取的保安措施*

60. 在調查過程中，專員注意到以下有關該電郵系統遠端存取的事項：

(i) 該電郵系統包括允許遠端存取的該網頁郵件服務。
(ii) 由該服務供應商提供的該網頁郵件服務不支援多重認證功能。
(iii) 沒有保安監察及警報功能以提示系統管理員任何來自異常或不明的 IP 位址查閱或登錄系統。
(iv) 沒有證據顯示有對該網頁郵件服務進行內部常規審核，或對資訊保安措施進行外部審核。

61. 在現今的商業運作中，由於許多機構採用混合工作模式結合在家工作與在辦公室工作，員工無法避免地需要遠端存取公司的網絡。專員認為機構在資訊保安方面應格外小心，以平衡員工從非工作地點查閱機構資源的相關風險。

62. 該網絡安全顧問公司在其調查報告中指出，由該服務供應商提供的該網頁郵件服務的保安功能未達企業級標準，缺乏多重認證及系統警示功能。

63. 日經亦表示由於他們非常依賴該服務供應商提供的服務及建議，因此未有就該電郵系統的保安功能性進行定期檢視。

64. 考慮到上述資料，包括該網絡安全顧問公司提供的調查報告，專員認為加入多重認證及系統警示功能可為遠端存取提供額外的防禦層。特別是多重認證功能使黑客更難以使用已盜取的密碼對該電郵系統進行未經授權的查閱，而系統監控和警示功能則可讓系統管理員採取更主動的行動以應對潛在的保安事故。

65. 專員亦認為日經應就該電郵系統的保安功能進行定期檢視，並定期考慮是否需要進行軟件升級或購置新產品來迎合日經的業務需求。

66. 日經亦向專員解釋選擇使用該電郵系統的原因是基於該服務供應商的規模和聲譽。然而，專員認為選擇任何資訊系統（包括電郵系統）的首要考慮因素應取決於系統所提供的功能及服務，包括供應商所提供的保安措施的種類，而非只是供應商的規模和聲譽。

(4) *欠缺針對資訊系統的保安措施*

67. 在調查過程中，專員注意到在該事件發生時，日經在資訊系統保安措施存在以下問題：

(i) 缺乏處理敏感個人資料（包括信用卡資料）的政策、程序和措施。

(ii) 缺乏對設置資訊保安工具的中央管理。每名員工都擁有隨意開啟或停用資訊保安工具的權限。

(iii) 缺乏管控措施以確保員工透過加密的渠道查閱其電郵帳戶，以防止密碼在不安全的網絡上被截取。

(iv) 缺乏密碼管控政策以確保預設的管理密碼不會被使用、不同帳戶設定不同的密碼，以及密碼應在預設的時限後更改，及具備指定的複雜性。

68. 正如專員已指出，負責任的資料使用者應時刻了解其資訊保安的狀況，制定充分有效的保安措施，包括安全政策和程序、安全管控措施以及日常內部和外部的審核，以保障其資訊系統。

69. 在衡量何謂足夠的資訊保安措施時，專員參考了政府資訊科技總監辦公室提供的網絡保安的良好行事方式[10]，其中包括：

(1) 使用多重機制鑑定用戶身份。

(2) 在網絡傳輸數據前，使用經證明有效的加密算法為數據加密。

(3) 強化防火牆和路由器，只容許在特定地點進行網絡管理工作，關閉不必要的網絡服務或使用加密通道進行網絡管理工作。

(4) 移除不必要的服務和軟件、及時修補系統的漏洞和取消沒被使用的帳戶，以保障伺服器的安全。

(5) 存取權應在有需要時才開啓及應定期進行檢視。

(6) 紀錄和定期檢視保安事宜：應備有記錄及審核功能以記錄網絡的連接情況，尤其是記錄未經授權的查閱，也應定期檢視這些紀錄。

(7) 建立保安管理的程序：如就保安事件記錄監測程序，改革管理程序或修補程式管理程序。

[10] https://www.infosec.gov.hk/tc/best-practices/business/securing-company-network

(8) 網絡／資訊保安管理員及支援職員以及用戶要接受培訓以確保他們可以遵從保安最佳作業守則和保安政策。

70. 與上述的基本保安措施相反，專員注意到日經沒有採取任何管控措施以規範敏感個人資料的處理。因此，日經接受客戶透過電郵提供信用卡資料以購買產品及服務，而保留於該電郵系統中的信用卡資料亦沒有被加密或以其他適當的方法保護。

71. 此外，專員注意到日經在關鍵時間未能符合上述指引建議的大部分保安措施的要求。專員認為這顯示日經缺乏資訊安全意識，以及日經在該事件之前未能採取所有切實可行的步驟以保障其持有的個人資料。

結論 — 違反保障資料第 4(1)原則

72. 專員注意到資料使用者根據保障資料第 4(1)原則保障其持有的個人資料的所需步驟在每一個案中都不盡相同，需要考慮許多因素，包括資料的數量、類別和敏感性；資料外洩可能導致的損害及傷害；企業管治和機構所採取的措施；以及與日經知名度相若的機構預期所應採用的技術政策、運營、控制和其他保安措施的合理質量和標準。

73. 專員認為日經應評估其員工收集、持有、處理及使用在該電郵系統內的客戶個人資料的相關風險，並按照保障資料第 4(1)原則採取所有切實可行的保安措施以保障其持有的個人資料。

74. 然而，根據調查所獲得的證據，該電郵系統在關鍵時間在保安方面明顯地存在以下不足：

(1) 薄弱的密碼管理；
(2) 保留已過時的電郵帳戶；
(3) 該電郵系統欠缺針對遠端存取的保安措施 ;及

(4) 欠缺針對資訊系統的保安措施。

75. 該事件揭示了日經沒有採取適當的保安政策、程序及措施以防範該電郵系統遭到網絡攻擊，導致黑客入侵該電郵系統令客戶的個人資料遭未經授權的查閱、處理或使用。**在本案中，專員認為日經未有採取所有切實可行的步驟保障其持有的客戶個人資料不受未獲准許的或意外的查閱、處理、刪除或使用所影響，因而違反了保障資料第 4(1)原則有關個人資料保安的規定。**

VI. 執法行動

76. 專員認為日經違反了《私隱條例》附表一的保障資料第 4(1) 原則，因此已根據《私隱條例》第 50(1)條所賦予的權力向日經送達執行通知，指示日經糾正以及防止有關違反再發生：

(1) 修訂資訊保安政策，加入並詳細說明強密碼管理政策、定期刪除已過期或不再使用的電郵帳戶機制，及訂立系統以定時監察及審核（包括內部審核）電郵帳戶的使用情況。

(2) 制訂有效措施以確保員工依循已修訂的資訊保安政策。

(3) 聘請獨立的資料保安專家對日經的系統保安，包括電郵系統進行定期檢視及審核。

(4) 為員工制定最新的資訊保安培訓，並妥善記錄培訓進度，以及對培訓的參與及有效程度作出評估。

(5) 由執行通知的日期起計兩個月內提供文件，證明已完成上述第 (1)至(4)項。

77. 根據《私隱條例》第 50A 條，資料使用者違反執行通知，即屬犯罪，一經首次定罪，最高可被判處第五級罰款（即港幣 50,000 元）及監禁兩年。

VII. 建議

78. 正如我們在本個案中所見，機構可以讓其員工使用互聯網收發電子郵件以進行有效的業務溝通，而其中一些電郵可能包含個人資料。專員希望藉此報告，提醒處理包含客戶個人資料的電郵的機構需加強警惕，以防止網絡攻擊影響其電郵系統。機構應制定適當的系統安全政策、措施和程序，並涵蓋以下領域。

(1) **設立個人資料私隱管理系統**：機構應建立及維持一套遵從《私隱條例》規定的系統，循規地使用個人資料。個人資料私隱管理系統有助機構管理由收集至銷毀個人資料的整個生命週期，令機構可迅速應對任何資料外洩事故，並確保遵從《私隱條例》。設立個人資料私隱管理系統可幫助機構贏得客戶及其他持份者的信任。

(2) **委任保障資料主任**：機構應委任員工負責監察《私隱條例》的遵從並向高級管理層匯報。保障資料主任的職責是把客戶關注的保障資料問題和涉及客戶個人資料事故的經驗納入機構的資料保障政策中，並安排提供相關培訓予員工以提升他們對個人資料保障的認知及知識。

(3) **電郵通訊政策**：機構應該對其持有的個人資料的種類以及允許員工透過電郵傳送資料的情況進行分類。機構亦應考慮限制敏感個人資料的只能由獲授權人員發送，並實施程序以確保只有獲授權人員才能保管及存取包含敏感個人資料的電郵。

(4) **保安措施**：如果機構允許通過電郵發送敏感的個人資料，可行的方法是在發送前對資料進行加密，以防止個人資料遭未經授權的攔截或存取。如收到載有未加密的敏感個人資料的電郵，應確保安全儲存資料。另外，當機構選擇電郵服務供應商時應

審視相關供應商所採取的保安措施，當中應包括有關軟件的系統保安，以及是否提供審計紀錄等。

(5) **工作場所的私隱友善文化**：員工應了解尊重及保護個人資料私隱，以及遵守《私隱條例》規定的重要性。他們應該在資料保障程序方面獲得足夠的培訓，並在處理含個人資料的電郵時格外留神。

－完－