南華體育會資料外洩事故的調查結果

根據香港法例第 486 章《個人資料（私隱）條例》第 48（2）條發表

背景

個人資料私隱專員公署（私隱專員公署）已就南華體育會（南華會）通報的一宗資料外洩事故完成調查。

調查源於南華會於 2024 年 3 月 18 日向私隱專員公署通報資料外洩事故，表示其伺服器遭勒索軟件攻擊及惡意加密（外洩事件）。

調查發現黑客早於 2022 年 1 月已在南華會一台與互聯網連接的伺服器內安裝了惡意程式，惟沒有證據顯示黑客當時有進一步的惡意活動。2024 年 3 月，黑客透過潛伏在相關伺服器內的惡意程式入侵南華會網絡並安裝遠端控制軟件，隨後透過遠端存取對南華會的電腦系統展開暴力攻擊，並進行其他惡意活動，包括網絡偵察、防禦規避、停用防毒及反惡意軟件、安裝憑證竊取工具及橫向移動，最終透過勒索軟件將載有會員個人資料的檔案加密。有關的勒索軟件屬 Trigona 的變種，外洩事件導致南華會共八台伺服器、一台數據儲存器及 18 台電腦遭受勒索軟件攻擊及加密。黑客曾要求南華會支付贖金，為已被加密的檔案解鎖。

受外洩事件影響的南華會會員數目為 72,315 名，所涉及的個人資料包括姓名、香港身份證號碼、護照號碼、相片、出生日期、地址、電郵地址、電話號碼及緊急聯絡人的姓名及電話號碼。

南華會在外洩事件發生後已通知所有受影響的會員，並採取一系列的改善措施以提升系統安全，包括限制南華會網內服務連接至互聯網、為管理員帳戶啟用多重認證功能、制訂密碼使用指引、定期掃描網絡以識別保安漏洞及全面執行資料離線備份等。

調查結果

經考慮外洩事件的情況及調查所獲得的資料，個人資料私隱專員（私隱專員）認為南華會的以下缺失是導致外洩事件發生的主因：—

1. **相關伺服器被意外地曝露於互聯網**，導致南華會的電腦系統遭受網絡攻擊的風險大幅增加，最終黑客透過相關伺服器作為踏板，入侵南華會網絡並進行勒索軟件攻擊；

2. **資訊系統欠缺有效的偵測措施**，以致南華會未能識別黑客早於 2022 年 1 月的惡意活動，讓黑客隨後於 2024 年 3 月透過潛伏在相關伺服器內的惡意程式入侵其網絡、遙距控制受入侵的電腦、設立具有管理員權限的帳戶、停用了安裝在相關伺服器內的防毒及反惡意軟件的功能，並於 3 月 15 至 16 日期間利用暴力攻擊合共向相關伺服器的另一管理員帳戶作出超過 43,400 次的登入嘗試，當中在 4 小時內更錄得超過 20,000 次的登入嘗試。由於南華會當時未有啟用密碼嘗試失敗的鎖定功能，導致黑客能不斷進行暴力攻擊；

3. **沒有為管理員帳戶啟用多重認證功能**，導致黑客無須經過其他身分核實程序便可進入相關伺服器的操作系統，進行各種惡意活動並加密會員的個人資料；

4. **欠缺資訊保安政策及指引**，因而未能提供全面及具體的資訊系統保安檢視規定及程序供員工依循。南華會亦沒有制訂書面密碼政策，包括列明密碼須有的複雜度、啟用密碼嘗試失敗的鎖定功能及更改密碼期限等措施，以保障帳戶安全；

5. **沒有定期進行風險評估及保安審計**，以檢視保安措施的成效，繼而採取改善措施以保護載有會員個人資料的系統免受網絡攻擊；及

6. **欠缺離線數據備份方案**，導致會員備份資料在外洩事件中同時被黑客加密，增加了數據復原的難度。

私隱專員的決定

基於上述原因，私隱專員認為南華會對保障所持有的會員個人資料意識薄弱。作為一個歷史悠久的體育團體及持有大量個人資料的機構，私隱專員對南華會在外洩事件發生前未能採取有效的資訊系統保安措施保障會員的個人資料安全感到非常失望。私隱專員認為，假如南華會在事發前已採取適當及足夠的機構性及技術性的保安措施，是次資料外洩事故是相當有機會可以避免的。因此，私隱專員裁定南華會沒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，違反了《個人資料（私隱）條例》的保障資料第 4（1）原則有關個人資料保安的規定。

私隱專員已向南華會送達執行通知，指示其採取措施以糾正違規事項，以及防止類似違規情況再次發生。

鍾麗玲
個人資料私隱專員
2024 年 10 月 22 日