# 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

## 香港銀行學會

## 伺服器遭勒索軟件攻擊

**報告編號：R23 - 6319**
**發表日期：2023 年 2 月 9 日**

# 調查報告：香港銀行學會
# 伺服器遭勒索軟件攻擊

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**
**2023 年 2 月 9 日**

# 目錄

# 調查報告

根據《個人資料（私隱）條例》第 48(2) 條發表

# 香港銀行學會
# 伺服器遭勒索軟件攻擊

## 摘要

### 背景

1. 2022 年 1 月 11 日，香港銀行學會（學會）向個人資料私隱專員公署（私隱專員公署）作出資料外洩事故通報，表示學會名下六台載有個人資料的伺服器（該些伺服器）遭勒索軟件攻擊及惡意加密，一名黑客威脅學會將該些伺服器內的檔案上載至互聯網，並要求學會支付贖金，為已被加密的檔案解鎖（該事件）。

2. 在接獲上述資料外洩事故通報後，私隱專員公署隨即對學會展開循規審查，以取得更多有關該事件的資料。在收到學會所提供的進一步資料後，個人資料私隱專員（專員）相信學會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 2022 年 5 月根據《私隱條例》第 38(b)條就該事件對學會展開調查。

### 調查所取得的資料及證據

3. 專員在進行調查過程中，審視及考慮了學會提供與該事件有關的資料，包括就學會對該些伺服器所採取的保安措施進行了四次的查

訊，並審視了學會委任的一間獨立資訊科技顧問公司提供的調查報告。專員亦考慮了學會在該事件發生後的跟進及補救工作。

## 該事件及相關的保安漏洞

4. 學會表示它於 2018 年 6 月向一間服務供應商（該服務供應商）購買一台防火牆（該防火牆），並分別於同年 6 月及 7 月安裝及啟用，以加強網絡安全。

5. 2019 年 5 月，該防火牆生產商在其網站發出保安建議（該建議），表示留意到有黑客披露其作業系統的漏洞。攻擊者可以通過相關漏洞繞過保安限制直接取得保密插口層虛擬私有網絡（Secure Sockets Layer Virtual Private Network, SSL VPN）帳戶名稱及密碼，並可於目標系統執行任何程式。根據該建議，該防火牆生產商呼籲用家立即停用 SSL VPN 功能，直至更新作業系統及重設所有帳戶密碼，同時建議啟用多重認證。

6. 政府電腦保安事故協調中心於 2019 年 8 月就相關漏洞發出高危保安警報，建議機構應立即為受影響的系統安裝修補程式。假如無法立即修補，應先停用 SSL VPN 直到已為受影響的系統進行修補。香港電腦保安事故協調中心隨後於 2020 年 12 月亦呼籲相關的本地網絡供應商及機構就相關漏洞盡快採取適當的補救措施。

7. 2021 年 1 月，學會因應本地 2019 冠狀病毒病疫情推行在家工作安排，遂啟用該防火牆的 SSL VPN 功能讓部份有需要的員工在家工作期間可以遙距登入其系統，惟事前未曾修補該防火牆相關漏洞。

8. 2021 年 12 月 30 日早上，學會的前線職員發現該些伺服器無法正常存取，資訊科技部門接獲通知後發現該些伺服器的檔案遭勒索軟件惡意加密。經初步調查後認為該些伺服器遭受網絡攻擊。其後發現除了該些伺服器外，學會的電腦及備份數據同樣遭勒索軟件加密。

## 受影響的個人資料

9. 學會估計該事件合共影響超過 13,000 名會員及約 10 萬名非會員的個人資料，當中涉及的個人資料除了姓名、聯絡資料、僱主名稱及職位外，部份人士的身份證號碼、信用卡號碼（不包括卡驗證碼）、出生日期、專業認證詳情及考試結果亦受影響。

## 資訊科技顧問公司的調查結果

10. 學會於該事件後立即委任了一間資訊科技顧問公司檢視其資訊系統安全。根據其調查報告，資訊科技顧問公司認為 (i) 學會未有制訂修補程式管理程序，以致未有為受影響的系統安裝修補程式，導致黑客利用相關漏洞首先取得 SSL VPN 帳戶名稱及密碼，並在入侵系統取得系統管理員權限後執行勒索軟件，最終成功加密該些伺服器，及 (ii) 學會未有為 SSL VPN 啟用多重認證。

## 學會對該事件的解釋

11. 學會向私隱專員公署表示該防火牆由該服務供應商負責保養，學會及該服務供應商直至該事件發生前並不知悉相關漏洞。此外，學會自 2018 年安裝該防火牆以來亦未曾接獲該服務供應商通知須為該防火牆安裝修補程式。學會並指出購買該防火牆時，同時包括由防火牆生產商提供的技術支援服務，但在該事件發生前未有從防火牆生產商獲悉相關漏洞的任何資訊。

12. 學會解釋雖然在該事件發生前其資訊科技部門共有 4 名員工（包括 1 名部門主管、2 名高級經理及 1 名高級主任），但由於日常營運及支援用戶的工作繁重，加上部門欠缺保養關鍵網絡設備的經驗，因此將有關工作外判予該服務供應商負責。

13. 學會亦承認在該事件發生前未曾對所有連接互聯網的伺服器、應用程式及端點裝置進行漏洞掃描，並指出該服務供應商未有建議學會

進行漏洞掃描。儘管如此，學會重申有持續監督該服務供應商的服務水平，並於每年續簽服務合約前由資訊科技部門經理作年度評估，並交由總經理及行政總裁確認及批核。

## 調查結果及違例事項

學會作為資料使用者

14. 學會在日常營運中，會收集、持有、處理及使用該些伺服器內的個人資料。因此，學會屬《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》附表一所列明的六項保障資料原則。

專員對該事件肇因的理解

15. 專員在審視資訊科技顧問公司的調查報告、學會對該事件的解釋，以及私隱專員公署在調查中獲得的所有資料後，同意調查報告的內容，認為事件源於學會未有制訂修補程式管理程序，以致未有為受影響的系統安裝修補程式，導致黑客利用相關漏洞首先取得 SSL VPN 帳戶名稱及密碼，在入侵系統取得系統管理員權限並執行勒索軟件後，成功加密該些伺服器；同時，學會亦未有為 SSL VPN 啟用多重認證，以加強相關系統保安。

學會違反保障資料第 4(1)原則

16. 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。

17. 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，專員認為學會在資料保安風險意識及個人資料保安措施方面存在明顯不

足，導致該些伺服器在可避免的情況下被黑客利用相關漏洞入侵系統並存取個人資料：—

**(1) 資料保安風險管理欠佳：**雖然學會表示其資訊科技部門欠缺保養關鍵網絡設備的經驗，因此將有關工作外判予該服務供應商負責，但專員認為學會在該事件發生前從未訂明資料保安風險管理機制，並要求服務提供者的行事方式遵從相關機制，對服務提供者的資料保安措施缺乏有效監察，做法欠佳。假如學會採取謹慎和盡職的態度，在服務合約中清楚訂明資料保安風險管理機制，要求服務提供者遵從指定機制定期進行保安檢查及漏洞掃描，應能及時發現相關漏洞對系統構成嚴重的潛在風險，並可盡早修補相關漏洞，從而避免該事件發生。

**(2) 資訊系統管理有欠妥善：**專員注意到在該事件發生時，學會在資訊系統保安措施方面存在以下問題：—

(1) 學會定期進行的滲透測試未有涵蓋網絡基礎設施及針對特定網絡攻擊的防禦能力；
(2) 系統安裝的防毒軟件僅具基本防護能力，未能有效抵禦勒索軟件攻擊；
(3) 系統未有安裝資料遺失防護系統，以偵測及阻止敏感資料被儲存至外置的儲存裝置，或是經電郵系統或互聯網被傳送到外界；
(4) 系統內部份帳戶的密碼強度不足，亦未有定期更改密碼，令有關帳戶容易被黑客攻擊入侵；及
(5) 其他資訊保安方面的缺失。

專員認為以上都反映了學會的個人資料保安管理有欠妥善，欠缺嚴謹措施規範員工行為及適時檢視系統設定，令載有個人資料的資訊系統的保安無法有效應對風險和威脅。

(3) **未適時啟用多重認證功能**：該防火牆生產商曾在 2019 年 5 月發出的建議提到，攻擊者可以透過相關漏洞繞過保安限制直接取得保密插口層虛擬私有網絡（Secure Sockets Layer Virtual Private Network, SSL VPN）帳戶名稱及密碼，並可於目標系統執行任何程式。該防火牆生產商因此呼籲用家立即停用 SSL VPN，直至更新作業系統及重設所有帳戶密碼，同時建議啟用多重認證功能。然而，學會在 2021 年 1 月啟用 SSL VPN 直至該事件發生時仍未有為 SSL VPN 實施多重認證功能，防止黑客利用外洩的密碼攻擊系統。

18. 在考慮本個案所有證據後，專員認為學會：—

(1) **沒有有效管理資料保安風險，包括未有制訂修補程式管理程序，導致沒有及時修補保安漏洞，讓黑客成功透過相關漏洞入侵系統，並加密該些伺服器；**
(2) **沒有妥善管理載有個人資料的資訊系統，包括滲透測試涵蓋面不足及系統欠缺有效的防毒軟件，導致系統無法抵禦黑客利用勒索軟件攻擊該些伺服器；及**
(3) **沒有跟從防火牆生產商的建議，在機構推行在家工作安排前為保密插口層虛擬私有網絡（SSL VPN）實施多重認證功能，防止黑客利用已獲取的密碼攻擊系統。**

19. **在本個案中，專員發現學會在資料保安風險管理及個人資料保安措施方面存在明顯不足，導致載有個人資料的伺服器遭勒索軟件攻擊。專員認為學會欠缺有效的資料保安風險管理機制，在保養關鍵的網絡設備上對服務提供者採取寬鬆態度，導致載有個人資料的資訊系統的保安措施無法有效應對網絡安全風險和威脅。總括來說，專員認為學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，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。**

20. 雖然學會在該事件中有需要改善之處，但專員樂見學會及時作出資料外洩通報，配合私隱專員公署的調查，並致力從該事件中汲取教訓。該事件發生後，學會通過採取多種機構性和技術性的改善措施，已經修補保安漏洞，提升整體系統保安以保障個人資料私隱。

## 執法行動

21. 專員已依據《私隱條例》第 50(1)條所賦予的權力，向學會送達執行通知，指示學會採取以下步驟以糾正違規情況，以及防止違規事件再發生：—

(1) 徹底檢視學會載有個人資料的系統保安，確保該些系統沒有已知的惡意軟件及保安漏洞；

(2) 聘請獨立的資料保安專家對學會的系統保安（包括載有個人資料的伺服器）進行定期檢視及審核；

(3) 修訂系統保安政策，明確訂定學會對其網絡設備（包括防火牆及伺服器）定期進行漏洞掃描；

(4) 修訂系統保安政策，明確訂定修補程式的管理政策及要求，並採取措施確保有關員工及提供系統保養服務的服務提供者依循相關政策及要求；及

(5) 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 (4)項指示。

## 建議

22. 專員希望藉此報告，向使用資訊及通訊科技處理個人資料的機構作出下述建議：—

(1) **提高警覺，防止黑客攻擊：**面對着不同的保安漏洞，機構應時刻提高警覺，定時進行風險評估，以檢視黑客攻擊對系統可能帶來的影響，並加以維護載有個人資料的系統例如伺服器、顧客資料庫等。

(2) **設立個人資料私隱管理系統：**機構應備有健全的個人資料私隱管理系統，循規使用及保留個人資料，有效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，以及贏得客戶及其他持份者的信任。

(3) **委任專責人員作為保障資料主任：**機構應明確制訂保障資料主任的角色及職責，包括監察遵從《私隱條例》的情況並向高級管理層匯報，以及把員工提出的保障資料事宜和涉及客戶個人資料外洩事故的經驗及教訓納入機構的培訓材料中。

(4) **提升資訊系統管理：**機構應制訂有效的修補程式管理程序，盡早修補保安漏洞，並因應系統載有的個人資料數量及敏感度採取相應的技術保安措施，例如連接虛擬私有網絡時啟用多重身份認證和登錄通知（如適用），為系統及帳戶帶來額外安全保障。另外，機構亦應定期查看日誌記錄，以及早識別異常的系統活動。

(5) **確實執行數據備份：**機構應制訂數據備份政策，定期備份含有重要資料的系統，並確保恢復機制能有效復原失去的或因惡意／勒索軟件而無法存取的資料。機構亦應根據資料的敏感度及重要性將數據分隔，並離線存放於安全地方，避免資料意外地喪失。

(6) **妥善監督服務提供者：**機構委聘資訊系統服務提供者維護網絡設備時，應該首先根據行業良好行事方式或作業指引制訂相關服務要求（例如需為機構的作業系統及軟件安裝關鍵的修補程式），並在服務合約中明文規定服務提供者遵從有關要求，作為日後監督服務提供者的依據。

## 其他評論

23. 繼2022年11月專員就一宗有關數據庫遭勒索軟件攻擊的事件發表調查報告後，本報告所涉及的調查已經是專員第二度就相關漏洞引致的資料保安事故進行的調查，這反映出機構若果未能盡早識別及處理保安漏洞，載有個人資料的資訊系統便很容易成為黑客攻擊的目標。

24. **專員認為機構不論規模大小，都應該從學會的資料保安事故中汲取教訓，應時刻留意最新的資訊系統保安資訊，並制定修補程式管理程序確保適時安裝軟件供應商所發布的保安修補程式。專員呼籲機構遵從《私隱條例》下個人資料保安的規定，採取所有切實可行的步驟保護其持有的個人資料安全，例如定期掃描可經互聯網接達的伺服器，檢查是否存在漏洞，並且時刻注意保安漏洞對載有個人資料的資訊系統可能造成的資料保安風險，盡早採取適當的補救行動。**

25. 專員藉此報告指出，穩健的資料保安系統是構成良好資料管治的一個重要元素。專員理解資料使用者所需採取的保護個人資料措施會因情況而異，資料使用者除了應諮詢專業資料保安專家和法律顧問，以確保遵從《私隱條例》的相關規定，亦可參考私隱專員公署出版的《資訊及通訊科技的保安措施指引》[1]，了解與資訊及通訊科技相關的資料保安措施建議及加強資料保安系統的良好行事方式。

[1] www.pcpd.org.hk//tc_chi/resources_centre/publications/files/guidance_datasecurity_c.pdf

# I. 背景

1. 2022 年 1 月 11 日，香港銀行學會（學會）向個人資料私隱專員公署（私隱專員公署）作出資料外洩事故通報，表示學會名下六台載有個人資料的伺服器（該些伺服器）遭勒索軟件攻擊及惡意加密，一名黑客威脅學會將該些伺服器內的檔案上載至互聯網，並要求學會支付贖金，為已被加密的檔案解鎖（該事件）。

2. 在接獲上述資料外洩事故通報後，私隱專員公署隨即對學會展開循規審查，以取得更多有關該事件的資料。在收到學會所提供的進一步資料後，個人資料私隱專員（專員）相信學會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 2022 年 5 月根據《私隱條例》第 38(b)[2]條就該事件對學會展開調查。

[2] 根據《私隱條例》第 38(b)條，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屬違反《私隱條例》下的規定，專員可就有關的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。

## II. 調查所取得的資料及證據

3. 專員在進行調查過程中，審視及考慮了學會提供與該事件有關的資料，包括就學會對該些伺服器所採取的保安措施進行了四次的查訊，並審視了學會委任的一間獨立資訊科技顧問公司提供的調查報告。專員亦考慮了學會在該事件發生後的跟進及補救工作。

學會背景及會籍計劃

4. 學會於 1963 年成立，是香港首家為銀行業提供培訓及認證的非牟利機構。學會的架構由議會及理事會組成，其成員包括香港銀行及金融業的代表及領袖[3]。

5. 學會設有個人、機構及關聯成員三種會籍架構。個人會籍是根據成員工作經驗及事業的不同階段分為六個級別[4]；機構會籍則供銀行、金融機構、監管機構及與銀行及金融服務業相關的組織申請[5]；至於非銀行金融機構（例如保險公司、信託公司等）及相關服務提供者（例如會計及法律機構、資訊科技服務供應商等）亦可申請成為關聯成員[6]。

6. 學會透過其網站不同類型的電子表格，例如會籍申請表、課程申請表、考試申請表、認證申請表等[7]收集申請人的個人資料。除上述各類表格外，學會亦會透過專用熱線或電郵收集申請人的個人資料，以跟進他們的查詢或投訴。

[3] www.hkib.org/storage/photos/shares/AR_Doc/2021_Taking_Flight_Widening_Services_&_Embracing_Digitalisation_for_Future_Talent.pdf#page=3

[4] www.hkib.org/page/45

[5] www.hkib.org/page/51

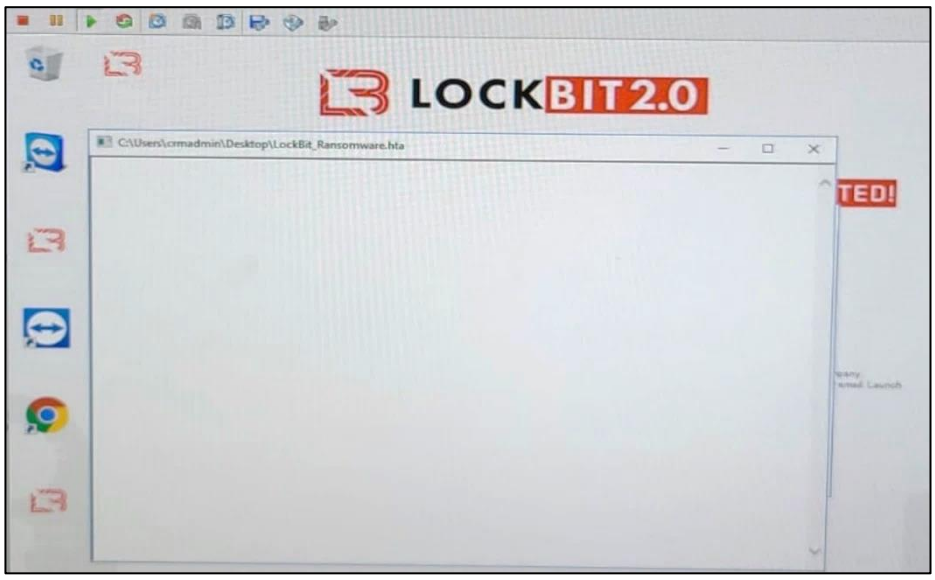
[6] www.hkib.org/page/173

[7] www.hkib.org/page/126

7. 根據學會 2021 年的年報，學會有接近 100 名機構會員及關聯成員，另有超過 13,000 名個人會員，當中九成屬具備銀行業資歷的專業會員[8]。

<u>該事件及相關的保安漏洞</u>

8. 2021 年 12 月 30 日早上，學會的前線職員發現該些伺服器無法正常存取，資訊科技部門接獲通知後發現該些伺服器的檔案遭勒索軟件惡意加密。經初步調查後認為該些伺服器遭受網絡攻擊。其後發現除了該些伺服器外，學會的電腦及備份數據[9]同樣遭勒索軟件加密。




學會提供其中一台被勒索軟件攻擊的伺服器截圖

9. 學會表示它於 2018 年 6 月向一間服務供應商（該服務供應商）購買一台防火牆（該防火牆），並分別於同年 6 月及 7 月安裝及啟用，以加強網絡安全。該服務供應商除了是該防火牆的分銷商，亦與學會簽訂服務合約，為學會辦公室的電腦及端點裝置提供硬件及軟件技術支援服務。

[8] www.hkib.org/storage/photos/shares/AR_Doc/2021_Taking_Flight_Widening_Services_&_Embracing_Digitalisation_for_Future_Talent.pdf#page=10

[9] 學會表示在該事件後發現負責備份數據的員工未有遵循其數據備份政策，將該些伺服器的資料進行離線備份，導致備份資料同遭勒索軟件惡意加密。

10. 2019年5月，該防火牆生產商在其網站發出保安建議（該建議）[10]，表示留意到有黑客披露其作業系統[11]的漏洞[12]。攻擊者可以通過相關漏洞繞過保安限制直接取得保密插口層虛擬私有網絡（Secure Sockets Layer Virtual Private Network, SSL VPN）[13]帳戶名稱及密碼，並可於目標系統執行任何程式。根據該建議，該防火牆生產商呼籲用家立即停用SSL VPN功能，直至更新作業系統及重設所有帳戶密碼，同時建議啟用多重認證。

11. 政府電腦保安事故協調中心於2019年8月就相關漏洞發出高危保安警報，建議機構應立即為受影響的系統安裝修補程式。假如無法立即修補，應先停用SSL VPN直到已為受影響的系統進行修補[14]。

12. 2020年11月，一名黑客在網上分享一份列表（該列表），列出超過49,000台尚未修補相關漏洞的設備的IP地址[15]。該防火牆生產商隨即於同月再度發文提醒用戶盡快安裝修補程式[16]。

13. 香港電腦保安事故協調中心隨後於2020年12月亦提醒各界該列表中有約1,000個IP地址來自香港，並呼籲相關的本地網絡供應商及機構就相關漏洞盡快採取適當的補救措施[17]。

[10] www.fortiguard.com/psirt/FG-IR-18-384

[11] 受影響的作業系統包括FortiOS 5.4.6至5.4.12、FortiOS 5.6.3至5.6.7及FortiOS 6.0.0至6.0.4。

[12] 根據香港電腦保安事故協調中心的保安公告，相關漏洞的識別碼為CVE-2018-13379。（www.hkcert.org/tc/security-bulletin/fortinet-fortos-multiple-vulnerabilities）

[13] SSL VPN讓用戶使用互聯網瀏覽器便可以加密通訊連接虛擬私有網絡裝置。（www.infosec.gov.hk/tc/best-practices/business/vpn-security）

[14] www.govcert.gov.hk/tc/alerts_detail.php?id=414

[15] 即互聯網規約地址

[16] www.fortinet.com/blog/psirt-blogs/update-regarding-cve-2018-13379

[17] www.hkcert.org/tc/blog/patch-fortios-ssl-vpn-vulnerability-cve-2018-13379-immediately

14. 2021 年 1 月，學會因應本地 2019 冠狀病毒病疫情推行在家工作安排，遂啟用該防火牆的 SSL VPN 功能讓部份有需要的員工[18]在家工作期間可以遙距登入其系統，惟事前未曾修補該防火牆相關漏洞。

受影響的個人資料

15. 學會估計該事件合共影響超過 13,000 名會員及約 10 萬名非會員的個人資料，當中涉及的個人資料除了姓名、聯絡資料、僱主名稱及職位外，部份人士的身份證號碼、信用卡號碼（不包括卡驗證碼）、出生日期、專業認證詳情及考試結果亦受影響，但學會亦估計該事件沒有給學會和受影響的個人（會員或非會員）造成直接經濟損失。

16. 由於學會的備份數據在該事件中同遭勒索軟件惡意加密，故此學會未能提供準確的受影響人數。此外，該些伺服器除了載有會員資料外，亦包括與專業認證考試及各類表格有關的資料，相信被惡意加密的檔案最早可追溯至 2002 年。

資訊科技顧問公司的調查結果

17. 學會於該事件後立即委任了一間資訊科技顧問公司檢視其資訊系統安全，並在調查過程中提交報告予私隱專員公署檢視。從資訊科技顧問公司的報告可見：—

(i) 學會未有制訂修補程式管理程序，以致未有為受影響的系統安裝修補程式，導致黑客利用相關漏洞首先取得 SSL VPN 帳戶名稱及密碼，並在入侵系統取得系統管理員權限後執行勒索軟件，最終成功加密該些伺服器；

(ii) 學會未有為 SSL VPN 啟用多重認證；及

[18] 學會表示在該事件發生時，學會 60 位員工中只有其中 10 位獲授權經該防火牆的 SSL VPN 功能遙距從其系統存取資料。

(iii) 資訊保安檢視識辨出一系列的缺失[19]，儘管沒有跡象顯示這些缺失直接引發該事件，當中包括：

(1) 學會定期進行的滲透測試未有涵蓋網絡基礎設施及針對特定網絡攻擊的防禦能力；
(2) 系統安裝的防毒軟件僅具基本防護能力，未能有效抵禦勒索軟件攻擊；
(3) 系統未有安裝資料遺失防護系統，以偵測及阻止敏感資料被儲存至外置的儲存裝置，或是經電郵系統或互聯網被傳送到外界；及
(4) 系統內部份帳戶的密碼強度不足，亦未有定期更改密碼。

學會對該事件的解釋

18. 學會向私隱專員公署表示該防火牆由該服務供應商負責保養，學會及該服務供應商直至該事件發生前並不知悉相關漏洞。此外，學會自 2018 年安裝該防火牆以來亦未曾接獲該服務供應商通知須為該防火牆安裝修補程式。學會並指出購買該防火牆時，同時包括由防火牆生產商提供的技術支援服務，但在該事件發生前未有從防火牆生產商獲悉相關漏洞的任何資訊。

19. 學會解釋雖然在該事件發生前其資訊科技部門共有 4 名員工（包括 1 名部門主管、2 名高級經理及 1 名高級主任），但由於日常營運及支援用戶的工作繁重，加上部門欠缺保養關鍵網絡設備的經驗，因此將有關工作外判予該服務供應商負責。

20. 學會亦承認在該事件發生前未曾對所有連接互聯網的伺服器、應用程式及端點裝置進行漏洞掃描，並指出該服務供應商未有建議學會進行漏洞掃描。儘管如此，學會重申有持續監督該服務供應商的服

[19] 為保障相關資訊系統安全的敏感資料，部份詳情被略去。

務水平，並於每年續簽服務合約前由資訊科技部門經理作年度評估，並交由總經理及行政總裁確認及批核。

跟進工作及補救措施

21. 該事件發生後，學會除了向私隱專員公署提交資料外洩事故通報外，並即時就該事件向警方報案。學會亦就該事件透過電郵、網站及／或電話通知受影響的會員及非會員。

22. 學會表示在獲悉資訊科技顧問公司的調查結果後，隨即指示該服務供應商更新該防火牆的作業系統以修補相關漏洞，並開啟該防火牆的日誌紀錄功能，以及為 SSL VPN 增設雙重認證功能。

23. 為了保障管理員及用戶帳戶安全，學會除了重設所有於該事件發生前的帳戶密碼外，亦重新檢視系統的密碼政策，強制所有帳戶必須定期更改密碼。

24. 因應資訊科技顧問公司在調查報告中所作的其他建議，學會採取了以下補救措施防止同類型事件再發生：—

(i) 限制應用程式經防火牆遠端從系統存取資料，並於端點裝置安裝程式偵測可疑的網絡傳輸，配合全天候監察服務提升防範網絡攻擊的能力；

(ii) 重建系統並提升網絡安全，增強網絡區隔[20]以減低網絡攻擊的影響，並於重建系統後進行網絡安全評估；

(iii) 更新與該服務供應商的服務合約，明文規定該服務供應商須定期檢查系統、固件及應用程式的更新、升級及可安裝的修補程式；

[20] 網絡區隔是指將網絡劃分為多個區段或子網絡，每個區段或子網絡都自成一個網絡，有助加強管理網絡流量及提升整體網絡的安全性。

(iv) 每年對系統進行保安檢查及漏洞掃瞄，同時訂閱香港電腦保安事故協調中心及勒索軟件資訊網站的通訊，以取得最新的勒索軟件攻擊情報及處理方法；

(v) 制訂數據備份和復原政策，並進行定期及突擊檢查確保員工按照數據備份政策進行離線及異地備份；及

(vi) 對其資訊保安系統進行了一系列的提升[21]，加強保障系統安全。

[21] 為保障相關資訊系統安全的敏感資料，有關詳情被略去。

## III. 調查結果及違例事項

學會作為資料使用者

25. 學會在日常營運中，會收集、持有、處理及使用該些伺服器內的個人資料。因此，學會屬《私隱條例》第 2(1)條釋義下的資料使用者[22]，須遵從《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。

保障資料第 4(1)原則

26. 《私隱條例》附表一保障資料第 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。

27. 在調查過程中，學會向私隱專員公署表示沒有足夠證據證實該事件導致個人資料外洩。然而，專員認為該名黑客利用相關漏洞存取載有個人資料的該些伺服器，表面已經構成未獲准許的查閱及／或處理個人資料的情況。

[22] 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*」。

28. 專員在審視資訊科技顧問公司的調查報告、學會對該事件的解釋，以及私隱專員公署在調查中獲得的所有資料後，同意調查報告的內容，認為事件源於學會未有制訂修補程式管理程序，以致未有為受影響的系統安裝修補程式，導致黑客利用相關漏洞首先取得 SSL VPN 帳戶名稱及密碼，在入侵系統取得系統管理員權限並執行勒索軟件後，成功加密該些伺服器；同時，學會亦未有為 SSL VPN 啟用多重認證，以加強相關系統保安。

29. 在此個案中，為了考慮學會是否符合保障資料第 4(1)原則的規定，專員會考慮學會在關鍵時間（即該事件發生時）對該些伺服器所採取的保安措施及學會如何處理資料保安風險。

30. 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，專員認為學會在資料保安風險意識及個人資料保安措施方面存在明顯不足，導致該些伺服器在可避免的情況下被黑客利用相關漏洞入侵系統並存取個人資料。

*(1) 資料保安風險管理欠佳*

31. 專員從學會委任的資訊科技顧問公司的調查報告中，注意到學會在該事件發生時未有制訂修補程式管理程序，以致未有為受影響的系統安裝修補程式，讓黑客成功透過相關漏洞入侵系統，並加密該些伺服器。調查報告亦指出學會定期進行的滲透測試未有涵蓋網絡基礎設施及針對特定網絡攻擊的防禦能力，令學會未能及早察覺該防火牆存在相關漏洞。

32. 專員認為防火牆屬保護系統的重要屏障，而黑客利用防火牆的相關漏洞取得帳戶名稱及密碼，性質形同密碼外洩，安全風險實在不容忽視。在本個案中，專員認為即使該防火牆生產商、政府電腦保安事故協調中心及香港電腦保安事故協調中心曾經再三提醒用戶修補相關漏洞，但學會及該服務供應商仍未察悉相關漏洞，可見學會及

該服務供應商的資料保安風險意識強差人意，缺乏有效的管理及檢討機制，以致未有妥善管理連接網絡的端點裝置。

33. 雖然學會表示其資訊科技部門欠缺保養關鍵網絡設備的經驗，因此將有關工作外判予該服務供應商負責，但專員認為學會在該事件發生前從未訂明資料保安風險管理機制，並要求服務提供者的行事方式遵從相關機制，對服務提供者的資料保安措施缺乏有效監察，做法欠佳。

34. 專員認為假如學會採取謹慎和盡職的態度，在服務合約中清楚訂明資料保安風險管理機制，要求服務提供者遵從指定機制定期進行保安檢查及漏洞掃描，應能及時發現相關漏洞對系統構成嚴重的潛在風險，並可盡早修補相關漏洞，從而避免該事件發生。專員認為學會並未有採取所有切實可行的步驟保障該些伺服器內的個人資料，承擔作為資料使用者的責任。

*(2) 資訊系統管理有欠妥善*

35. 另一方面，儘管學會重申其資訊科技部門每月初均會對伺服器及數據備份進行例行檢查，確保伺服器及數據備份狀態正常，但專員從學會委任的資訊科技顧問公司的調查報告中注意到在該事件發生時，學會在資訊系統保安措施方面存在以下問題：—

(1) 學會定期進行的滲透測試未有涵蓋網絡基礎設施及針對特定網絡攻擊的防禦能力；
(2) 系統安裝的防毒軟件僅具基本防護能力，未能有效抵禦勒索軟件攻擊；
(3) 系統未有安裝資料遺失防護系統，以偵測及阻止敏感資料被儲存至外置的儲存裝置，或是經電郵系統或互聯網被傳送到外界；

(4) 系統內部份帳戶的密碼強度不足，亦未有定期更改密碼，令有關帳戶容易被黑客攻擊入侵；及

(5) 其他資訊保安方面的缺失[23]。

36. 雖然沒有跡象顯示這些缺失直接導致該事件發生，但專員認為以上都反映了學會的個人資料保安管理有欠妥善，欠缺嚴謹措施規範員工行為及適時檢視系統設定，令載有個人資料的資訊系統的保安無法有效應對風險和威脅。

*(3) 未適時啟用多重認證功能*

37. 該防火牆生產商曾在 2019 年 5 月發出的建議提到，攻擊者可以透過相關漏洞繞過保安限制直接取得保密插口層虛擬私有網絡（Secure Sockets Layer Virtual Private Network, SSL VPN）帳戶名稱及密碼，並可於目標系統執行任何程式。該防火牆生產商因此呼籲用家立即停用 SSL VPN，直至更新作業系統及重設所有帳戶密碼，同時建議啟用多重認證功能。然而，學會在 2021 年 1 月啟用 SSL VPN 直至該事件發生時仍未有為 SSL VPN 實施多重認證功能，防止黑客利用外洩的密碼攻擊系統。

38. 專員認為根據該防火牆生產商的建議，以及學會讓部份員工在在家工作期間透過 SSL VPN 遙距連接學會系統的情況下，學會理應啟用多重認證功能以提升保安措施及保障其載有個人資料的系統安全。在該事件中，學會容許載有個人資料的資訊系統曝露在資料保安風險中，是導致該些伺服器在可避免的情況下仍遭勒索軟件攻擊的主要原因。

39. 在衡量何謂足夠的資料保安措施時，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[24]，當中包括：—

[23] 為保障相關資訊系統安全的敏感資料，有關詳情被略去。

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

(1) 在網絡設計時加入保安的考慮：所有保安事項，例如管理政策，技術訓練和外判要求應該早在網絡設計階段開始考慮。

(2) 將伺服器設定至較佳的保安狀態：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。

(3) 加強應用程式的保安：安裝保安修補程式、強化應用程式的設定或鎖上應用程式運作的環境。

(4) 建立保安管理的程序：例如保安事件紀錄監測程序，改革管理程序或修補程式管理程序。

(5) 職員培訓：網絡／資訊保安管理員及支援職員以及一般員工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。

40. 專員注意到學會在該事件發生時未能符合上述指引建議的大部份保安措施的要求，以保障其載有個人資料的伺服器免受黑客攻擊。

結論：違反保障資料第 4(1)原則

41. 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；資料管治和機構所採取的措施；以及相類似機構合理預期所應採用的資訊科技政策、運作、控制和其他保安措施的質量和標準。

42. 專員認為學會作為在銀行業具代表性的資料使用者，持有大量銀行從業員的個人資料，理應就收集、持有、處理及使用這些資料制訂完善的政策、進行適當的風險評估，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，以確保由其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。

43. 在考慮本個案所有證據後，專員認為學會：—

(1) 沒有有效管理資料保安風險，包括未有制訂修補程式管理程序，導致沒有及時修補保安漏洞，讓黑客成功透過相關漏洞入侵系統，並加密該些伺服器；

(2) 沒有妥善管理載有個人資料的資訊系統，包括滲透測試涵蓋面不足及系統欠缺有效的防毒軟件，導致系統無法抵禦黑客利用勒索軟件攻擊該些伺服器；及

(3) 沒有跟從防火牆生產商的建議，在機構推行在家工作安排前為保密插口層虛擬私有網絡（**SSL VPN**）實施多重認證功能，防止黑客利用已獲取的密碼攻擊系統。

44. 在本個案中，專員發現學會在資料保安風險管理及個人資料保安措施方面存在明顯不足，導致載有個人資料的伺服器遭勒索軟件攻擊。專員認為學會欠缺有效的資料保安風險管理機制，在保養關鍵的網絡設備上對服務提供者採取寬鬆態度，導致載有個人資料的資訊系統的保安措施無法有效應對網絡安全風險和威脅。總括來說，專員認為學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，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。

45. 雖然學會在該事件中有需要改善之處，但專員樂見學會及時作出資料外洩通報，配合私隱專員公署的調查，並致力從該事件中汲取教訓。該事件發生後，學會通過採取多種機構性和技術性的改善措施，已經修補保安漏洞，提升整體系統保安以保障個人資料私隱。

# IV. 執法行動

46. 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。

47. 專員認為學會違反了《私隱條例》附表一的保障資料第 4(1) 原則，因此依據《私隱條例》第 50(1)條所賦予的權力向學會送達執行通知，指示學會採取以下步驟以糾正違規情況，以及防止違規事件再發生：—

(1) 徹底檢視學會載有個人資料的系統保安，確保該些系統沒有已知的惡意軟件及保安漏洞；

(2) 聘請獨立的資料保安專家對學會的系統保安（包括載有個人資料的伺服器）進行定期檢視及審核；

(3) 修訂系統保安政策，明確訂定學會對其網絡設備（包括防火牆及伺服器）定期進行漏洞掃描；

(4) 修訂系統保安政策，明確訂定修補程式的管理政策及要求，並採取措施確保有關員工及提供系統保養服務的服務提供者依循相關政策及要求；及

(5) 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 (4)項指示。

48. 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。

# V. 建議及其他評論

49. 《私隱條例》第 48(2)條訂明，專員在完成一項調查後，如認為是符合公眾利益，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及其他評論。專員除了根據《私隱條例》第 50(1)條就伺服器遭勒索軟件攻擊一事向學會送達執行通知外，亦希望藉此報告，向使用資訊及通訊科技處理個人資料的機構作出下述建議。

## 提高警覺，防止黑客攻擊

50. 面對着不同的保安漏洞，機構應時刻提高警覺，定時進行風險評估，以檢視黑客攻擊對系統可能帶來的影響，並加以維護載有個人資料的系統例如伺服器、顧客資料庫等。

## 設立個人資料私隱管理系統

51. 機構應備有健全的個人資料私隱管理系統，循規使用及保留個人資料，有效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，以及贏得客戶及其他持份者的信任。

## 委任專責人員作為保障資料主任

52. 機構應明確制訂保障資料主任的角色及職責，包括監察遵從《私隱條例》的情況並向高級管理層匯報，以及把員工提出的保障資料事宜和涉及客戶個人資料外洩事故的經驗及教訓納入機構的培訓材料中。

### 提升資訊系統管理

53. 機構應制訂有效的修補程式管理程序，盡早修補保安漏洞，並因應系統載有的個人資料數量及敏感度採取相應的技術保安措施，例如連接虛擬私有網絡時啟用多重身份認證和登錄通知（如適用），為系統及帳戶帶來額外安全保障。另外，機構亦應定期查看日誌記錄，以及早識別異常的系統活動。

### 確實執行數據備份

54. 機構應制訂數據備份政策，定期備份含有重要資料的系統，並確保恢復機制能有效復原失去的或因惡意／勒索軟件而無法存取的資料。機構亦應根據資料的敏感度及重要性將數據分隔，並離線存放於安全地方，避免資料意外地喪失。

### 妥善監督服務提供者

55. 機構委聘資訊系統服務提供者維護網絡設備時，應該首先根據行業良好行事方式或作業指引制訂相關服務要求（例如需為機構的作業系統及軟件安裝關鍵的修補程式），並在服務合約中明文規定服務提供者遵從有關要求，作為日後監督服務提供者的依據。

## 其他評論

56. 繼 2022 年 11 月專員就一宗有關數據庫遭勒索軟件攻擊的事件發表調查報告[25]後，本報告所涉及的調查已經是專員第二度就相關漏洞引致的資料保安事故進行的調查，這反映出機構若果未能盡早識別及處理保安漏洞，載有個人資料的資訊系統便很容易成為黑客攻擊的目標。

[25] www.pcpd.org.hk/tc_chi/enforcement/commissioners_findings/files/r22_18947_c.pdf

57. **專員認為機構不論規模大小，都應該從學會的資料保安事故中汲取教訓，應時刻留意最新的資訊系統保安資訊，並制定修補程式管理程序確保適時安裝軟件供應商所發布的保安修補程式。專員呼籲機構遵從《私隱條例》下個人資料保安的規定，採取所有切實可行的步驟保護其持有的個人資料安全，例如定期掃描可經互聯網接達的伺服器，檢查是否存在漏洞，並且時刻注意保安漏洞對載有個人資料的資訊系統可能造成的資料保安風險，盡早採取適當的補救行動。**

58. 隨着資料數碼化趨勢加速、資訊及通訊科技的互聯互通，以及資料本身的價值不斷上升，個人資料保安的風險亦隨之而增加。近年在香港和其他司法管轄區所發生的資料保安事故之上升趨勢亦證明了這一點。不論資料使用者是中小企業還是跨國企業，資料保安事故都可在聲譽及財務兩方面為其帶來嚴重後果。

59. 專員藉此報告指出，穩健的資料保安系統是構成良好資料管治的一個重要元素。專員理解資料使用者所需採取的保護個人資料措施會因情況而異，資料使用者除了應諮詢專業資料保安專家和法律顧問，以確保遵從《私隱條例》的相關規定，亦可參考私隱專員公署出版的《資訊及通訊科技的保安措施指引》[26]，了解與資訊及通訊科技相關的資料保安措施建議及加強資料保安系統的良好行事方式。

－完－

[26] www.pcpd.org.hk//tc_chi/resources_centre/publications/files/guidance_datasecurity_c.pdf