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

香港數碼港管理有限公司

資訊系統遭勒索軟件攻擊

報告編號：R24 – 12170
發表日期：2024 年 4 月 2 日

調查報告：香港數碼港管理有限公司
資訊系統遭勒索軟件攻擊

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
2024 年 4 月 2 日

調查報告

根據《個人資料（私隱）條例》第 48(2) 條發表

香港數碼港管理有限公司
資訊系統遭勒索軟件攻擊

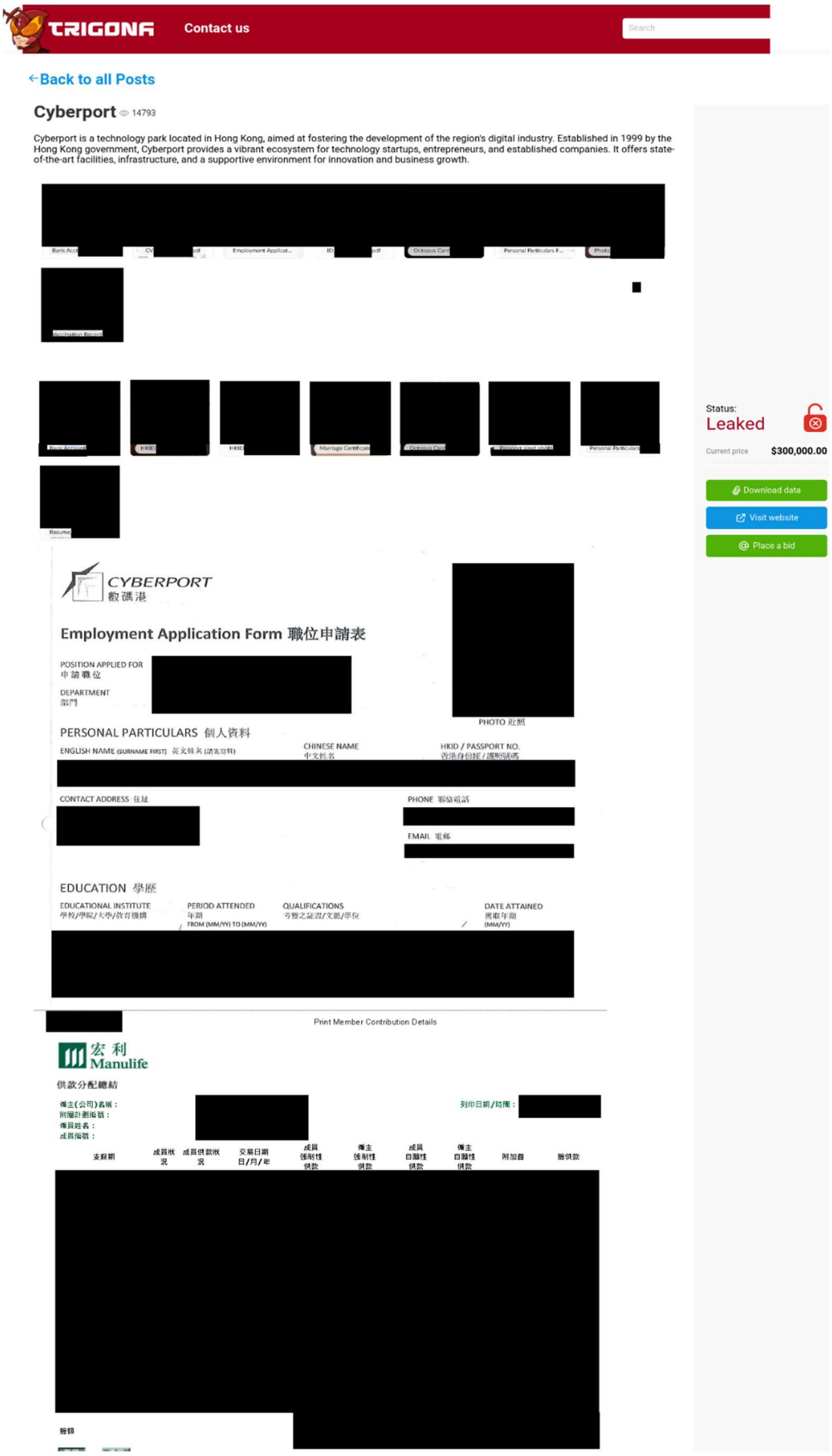
I. 背景

1. 2023 年 8 月 18 日，香港數碼港管理有限公司（數碼港）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，表示其電腦系統及檔案伺服器遭受到勒索軟件攻擊及惡意加密。自稱 Trigona 的黑客組織要求數碼港支付贖金，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數碼港展開循規審查，以取得更多有關該事件的資料，並建議數碼港盡快通知所有受影響人士。

3. 2023 年 9 月 5 日，有網絡安全平台發現黑客組織 Trigona 於其網頁聲稱已取得數碼港的數據，當中涉及超過 400GB 的數據，並公開部分數據範本以供出售。數碼港隨後分別於 2023 年 9 月 6 及 12 日就該事件發布新聞稿，確認有未經授權的第三方入侵數碼港部分的電腦系統，以及講述其跟進行動，包括關閉受影響的電腦設備及委聘獨立的網絡安全專家（網絡安全專家）進行調查。

4. 下圖顯示黑客組織 Trigona 網頁上的銷售訊息（已遮蓋載有個人資料的內容）：



5. 在收到數碼港提供的進一步資料後，個人資料私隱專員（專員）隨即依據既定機制根據香港法例第 486 章《個人資料（私隱）條例》（《私隱條例》）第 38(b)條[1]就該事件對數碼港展開調查，以確定數碼港在該事件中的作為或行為是否涉及違反《私隱條例》的規定。同時，專員亦再次發信要求數碼港盡快通知所有受影響人士。

II. 調查所得的資料

6. 調查在 2023 年 9 月至 2024 年 3 月期間進行。在調查過程中，專員檢視了上載於暗網的數據範本，並就數碼港在該事件發生時採取的保安措施共進行了四次查訊，亦審視了數碼港提供與該事件有關的各種資料，包括由數碼港委聘的網絡安全專家提供的調查報告。專員亦考慮了數碼港在該事件發生後發出的新聞稿、跟進及補救工作。

7. 根據數碼港提供的資料，以下為與該事件有關的主要事項：

日期	事件
2023 年 8 月 6 日	黑客利用具管理員權限的帳戶進入數碼港的網絡。
2023 年 8 月 14 日	數碼港伺服器內的檔案遭受到勒索軟件攻擊及惡意加密。
2023 年 8 月 14 日	數碼港採取補救行動，包括更改所有帳戶密碼。
2023 年 8 月 17 日	數碼港接獲黑客的勒索訊息。
2023 年 8 月 18 日	數碼港伺服器內的檔案再次遭受到勒索軟件攻擊及惡意加密。
2023 年 8 月 18 日	數碼港就該事件向私隱專員公署作出資料外洩事故通報，私隱專員公署隨即就該事件展開循規審查，並建議數碼港盡快通知所有受影響人士。

[1] 根據《私隱條例》第 38(b)條，凡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，以確定有關作為或行為是否屬違反《私隱條例》下的規定。

8. 根據數碼港於其網站的描述，數碼港由香港特別行政區政府全資擁有，管理作為香港數碼科技旗艦及創業培育基地的數碼港園區，匯聚超過 2,000 間社群企業，包括超過 900 間駐園區及接近 1,100 間非駐園區的初創企業和科技公司。

受影響的個人資料

9. 根據《私隱條例》第 2(1)條，「個人資料」是指任何直接或間接與一名在世的個人有關的資料，而從該資料直接或間接地確定有關的個人的身份是切實可行的；及該資料的存在形式令予以查閱及處理均是切實可行的。

10. 數碼港表示共 13,632 名資料當事人受該事件影響，包括近 8,000 名與僱傭有關的人士[2]，並確認其中 5,292 名求職者及離職僱員的個人資料[3]已被保留超過保留期限。其他受該事件影響的人士包括數碼港的管理人員、酒店職員、資助計劃實習生，以及與數碼港有業務往來的人士[4]。

11. 綜合數碼港提供的資料及專員檢視上載於暗網的數據範本所得，受該事件影響的個人資料除了姓名、身份證號碼及／或副本、護照號碼及／或聯絡資料外，還有部份人士的財務資料[5]、健康資料[6]、照片、出生日期、僱傭資料、社交媒體帳戶資料及／或學歷資料及屬數位人士的信用卡資料[7]等亦受影響。

網絡安全專家的調查結果

12. 數碼港於該事件後委聘了網絡安全專家調查該事件，並於 2024 年 2 月中提交調查報告予私隱專員公署檢視。有關調查報告指出是次網絡攻擊的起因是由於黑客取得數碼港一個具管理員權限的帳戶憑證，並透過遠端桌面連接進入數碼港的網絡。

[2] 包括求職者、現職及離職僱員，以及他們的諮詢人、配偶及／或受供養人等。
[3] 包括身份證號碼、出生日期、銀行帳戶資料、聯絡資料、僱傭資料及／或學歷資料。
[4] 包括收款人、投標者聯絡人及租約簽署人等。
[5] 例如銀行帳戶號碼。
[6] 例如醫療報告。
[7] 數碼港指部分信用卡已失效。

13. 調查報告亦指出黑客進入數碼港的網絡後，透過各種工具進行網絡內部的橫向移動、防禦規避、資料竊取及放置勒索軟件等惡意活動。數碼港的多個伺服器及網絡儲存裝置在該事件中被入侵，涉及 13 個 Windows 系統及兩台虛擬伺服器。

14. 該網絡安全專家在報告中向數碼港的資訊系統保安列出了 16 項建議，而數碼港已完成當中 15 項建議[8]，當中包括升級其端點保護軟件，並聘請第三方顧問進行主動網路安全監控和滲透測試。

III. 調查結果及違例事項

數碼港作為資料使用者

15. 數碼港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。

《私隱條例》的相關規定

16. 保障資料第 2(2)原則訂明，資料使用者須採取所有切實可行的步驟，以確保個人資料的保存時間不超過將其保存以貫徹該資料被使用於或會被使用於的目的（包括任何直接有關的目的）所需的時間。

17. 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；

[8] 為保障相關資訊系統安全的敏感資料，本報告略去有關詳情。

(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。

<u>調查結果</u>

18. 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的缺失導致：—

(1) 資訊系統欠缺有效的偵測措施

19. 根據調查所得的資料，黑客透過暴力攻擊[9]取得數碼港一個具管理員權限的帳戶憑證，並使用這個帳戶透過遠端桌面連接進入數碼港的網絡。在成功進入數碼港的網絡後，黑客再次透過暴力攻擊及轉儲憑證[10]等方法取得另外三個具管理員權限的帳戶[11]的控制權，以部署進行各種網絡內部的橫向移動及防禦規避[12]等活動，繼而對相關的伺服器及網絡儲存裝置進行兩次的勒索軟件攻擊及惡意加密，並竊取資料。

20. 明顯地，黑客成功透過暴力攻擊取得該個具管理員權限的帳戶憑證，是這次網絡攻擊的起點。然而，由 2023 年 8 月 6 日黑客進入數碼港的網絡起，直至黑客於 8 月 14 日對數碼港的網絡進行勒索軟件攻擊的期間，由於黑客使用具權限的帳戶在網絡中活動，數碼港未能偵測黑客的入侵及其相關的惡意活動。

[9] 暴力攻擊是通過試誤法以破解憑證，反覆試驗所有可能的組合，直至猜到正確密碼。
[10] 於系統取得當中儲存的用戶憑證（例如登入名稱及密碼）的方法。
[11] 該些具管理員權限的帳戶可繞過防火牆的保護及停止反惡意軟體程式的運作。
[12] 終止系統防衛軟件或相關服務的技術。

21. 數碼港表示在事發時其資訊系統安裝了一款反惡意軟體程式，以偵測網絡中的可疑活動，但由於黑客取得管理員權限，黑客成功停止了該反惡意軟體程式的功能。數碼港確認上述情況發生之後，已沒有其他措施或工具足以偵測其網絡中的可疑活動。

22. 專員認為數碼港作為一間使用具規模的資訊系統以儲存大量個人資料的機構，僅依賴一款反惡意軟體程式來偵測異常活動明顯是不足夠及不成比例。專員認為，為確保資訊系統安全及數據安全，不論規模大小的機構均應採用多層防禦策略[13]，包括配置端點保護解決方案、實施入侵偵測和預防系統等，以更有效地偵測網絡中的可疑活動。專員注意到數碼港於該事件後已於其資訊系統部署更多的偵測工具，以偵測並封鎖惡意檔案及識辨入侵指標，可見這些事後的安排對數碼港而言是切實可行的。若然數碼港當初部署足夠的工具以偵測及預防網絡攻擊，便有相當機會在黑客進行最初的暴力攻擊時或入侵的初期察覺其活動，從而可以避免其後的資料竊取及其他惡意活動。

(2) 未有為遠端存取資料啟用多重認證功能

23. 如前段所述，黑客透過暴力攻擊取得數碼港一個具管理員權限的帳戶憑證，並使用這個帳戶透過遠端桌面連接進入數碼港的網絡。數碼港確認在事發時未有啟用多重認證功能，以核實獲授權可遠端登入數碼港網絡的用戶的身分。數碼港表示已於 2023 年 11 月配備新的虛擬私有網路[14]閘道，當中設置了多重認證功能。

24. 專員認為，為保障機構的網絡安全及數據安全，尤其當機構允許用戶以遠端連接其電腦系統時，機構應選擇一套能夠支援雙重認證或多重認證的軟件，並設置一組強密碼，亦要保持遠端桌面控制軟件為最新版本。在該事件中，若然數碼港有為遠端存取資料啟用多重認證功能以確認該具管理員權限的帳戶的用戶身分，這便可能阻止黑客透過該帳戶進入數碼港的網絡，從而放置勒索軟件並竊取系統當中儲存的個人資料。

[13] 泛指使用多種安全措施來建構縱深防禦，屬網絡保安的基本概念。
[14] Virtual private network

25. 因此，數碼港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數碼港網絡的用戶的身分，是導致其資訊系統在可避免的情況下遭勒索軟件攻擊的重要原因。

(3) 對資訊系統進行的保安審計不足

26. 數碼港表示會每兩年對其資訊系統進行保安審計，以評估數碼港的所有資訊系統有否存在保安漏洞。然而，在該事件發生前最後的一次保安審計於 2021 年尾進行，即已超過 19 個月。此外，數碼港指出受該事件影響的其中一個系統於 2022 年第三季推出，因此 2021 年進行的保安審計未有涵蓋該系統，數碼港亦確認未有為該系統進行風險評估或獨立的保安審計。

27. 在現今的數碼年代，網絡攻擊漸見頻繁，而攻擊手法亦日新月異，因此除安裝合適的保安工具並適時更新外，定期檢視機構的整體網絡安全（包括保安審計）亦是必須的。資訊科技保安審計是以資訊科技保安政策或標準為基礎的遵行狀況審計，以確定現有保護的整體情況，並驗證現有的保護措施是否已經妥善地實行。保安審計應在不同情況下進行，包括在啟用嶄新或經過重大升級的系統之前。考慮到現時網絡攻擊的情況及數碼港的資訊系統的規模，專員認為數碼港每兩年進行保安審計的頻率實屬不足，未能適時應對資訊科技的變化及網絡安全的風險。此外，數碼港沒有規定對其中一個受影響的系統在啟用前進行風險評估或獨立的保安審計，更是一個明顯的缺失。

28. 換言之，若然數碼港進行更頻繁的保安審計，並在啟用受事件影響的系統之前進行適當的風險評估或獨立的保安審計，則可以增加數碼港的資訊系統的保安屏障，例如審計結果可令數碼港注意到應設置多重認證功能及安裝足夠的偵測措施，這可能避免是次資料外洩事故的發生。

(4) 資訊保安政策有欠具體

29. 就有關資訊保安方面的書面政策及程序，數碼港向專員提供了一份「數碼港資訊保安政策」[15]（該政策）。該政策合共 41 頁，而與網絡保安較為有關的部分主要見於「外部查閱保安政策」[16]及「惡意程式碼（病毒）政策」[17]，各佔該政策的兩頁。雖然該政策訂明數碼港在運作層面須按需要為特定的保安要求制訂工作程序，惟數碼港未有進一步向專員提供有關的工作程序或指引。

30. 專員在審視該政策後認為，在網絡保安方面，該政策主要提供了一些一般性的原則，而個別要求有欠具體，例如就「有合適的病毒保護措施」及「進行定時的病毒感染檢查」，該政策並未對何謂合適及定時有所着墨。專員認為，數碼港在制訂資訊保安政策時，除訂明原則性的保安措施外，亦應提供更具體的操作程序及／或指引，以清晰地涵蓋各項有關使用保安工具及進行保安審計等的規定，讓員工有一個具體的網絡保安框架可依循，從而提升資訊安全，防範黑客的攻擊。

(5) 不必要地保留個人資料

31. 在調查的過程中，數碼港確認部分受該事件影響的個人資料已被保留超過保留期限，當中包括 5,292 名求職者及離職僱員的個人資料。根據數碼港提供的資料保留政策，求職者的個人資料會保留一年，而僱員的個人資料則會於受僱其間保留。然而，數碼港未能解釋在有關保留期限屆滿後仍保留上述人士的個人資料的原因。

32. 專員認為，機構在收集個人資料後，需根據其資料保留政策考慮保留資料的期限，並制訂相應措施確保適時刪除已屆保留期限的資料，以避免不必要地或過長地保留個人資料，從而增加資料外洩的風險。

[15] Cyberport Information Security Policy
[16] External Access Security Policy
[17] Malicious Code (Virus) Policy

33. 專員注意到數碼港沒有根據其資料保留政策在保留期限屆滿後刪除其收集得的個人資料，亦未能解釋保留該些資料的原因，導致受該事件影響的 13,632 名資料當事人當中，約四成人士因其個人資料被不必要地保留而被該事件影響。若然數碼港當初採取切實可行的步驟，刪除已屆保留期限的資料，受該事件影響的人數便會大幅減少。

違反《私隱條例》保障資料第 4(1)及 2(2)原則

34. 在考慮本個案的所有證據後，專員認為數碼港須為下列缺失負責：

(1) 數碼港的資訊系統欠缺有效的偵測措施，導致未能有效地偵測黑客以暴力攻擊其資訊系統，令黑客能成功獲取具管理員權限的帳戶憑證，並繼而進行勒索軟件攻擊及竊取儲存於系統內的個人資料；
(2) 數碼港沒有為遠端存取資料啟用多重認證功能，導致黑客能利用獲取得的帳戶憑證透過遠端桌面連接進入數碼港的網絡，竊取個人資料；
(3) 數碼港對資訊系統進行的保安審計不足，未能適時應對資訊科技的變化及網絡安全的風險；
(4) 數碼港的資訊保安政策有欠具體，未能讓員工有一個具體的網絡保安框架可依循；及
(5) 數碼港沒有根據其資料保留政策在保留期屆滿後刪除其收集得的個人資料，導致約四成受影響人士因其個人資料被不必要地保留而受該事件影響。

35. 基於上述情況，專員認為數碼港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。

36. 此外，專員認為數碼港未有採取所有切實可行的步驟，以確保個人資料的保存時間不超過使用該資料實際所需的時間，因而違反了保障資料第 2(2)原則有關個人資料保留的規定。

總結

37. 專員認為數碼港是一間具規模的機構，恆常地持有並處理大量不同人士的個人資料，持份者及公眾會合理地期望數碼港投入足夠資源確保其資訊系統及數據的安全。因此，數碼港應採取足夠的機構性及技術性的保安措施，以保障載有個人資料的資訊系統的安全，從而符合持份者及公眾的期望。然而，調查顯示數碼港在該事件發生之前未有採取足夠及有效的措施以保障其資訊系統的安全，亦未有及時根據其資料保留政策刪除已屆保存期限的資料，因而違反了《私隱條例》有關個人資料保留及保安的規定。

38. 另一方面，專員樂見數碼港及時作出資料外洩通報，配合私隱專員公署的調查。該事件發生後，數碼港已採取多種機構性和技術性的改善措施，提升整體系統保安以保障個人資料私隱，如實施網絡安全專家提出的資訊系統保安建議，以及防止類似事件再次發生的綜合措施整體路線圖。專員期望數碼港從該事件中汲取教訓，建立重視數據安全的企業文化，並時刻提高警覺，定期進行風險評估，以檢視黑客攻擊及其他各種網絡保安威脅對載有個人資料系統可能帶來的影響。

IV. 執法行動

39. 專員已依據《私隱條例》第 50(1)條所賦予的權力，向數碼港送達執行通知，指示數碼港採取以下步驟以糾正違規情況，以及防止類似違規事件再發生：—

(1) 徹底檢視數碼港載有個人資料的資訊系統的安全及其保安措施，確保該些系統沒有已知的惡意軟件及保安漏洞以及具備有效的偵測措施；

(2) 為所有會存取載有個人資料的數碼港資訊系統的遙距使用者實施多重身分認證，並定期檢視遙距存取的權限；

(3) 聘請獨立的資訊保安專家對數碼港的資訊系統進行最少每年一次的風險評估及保安審計；

(4) 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，及進行風險評估及保安審計的要求；

(5) 從數碼港資訊系統銷毀所有逾期保留的個人資料；

(6) 制訂清晰的資料保留政策，訂明每個數碼港系統內個人資料的保留期限，及制訂刪除已屆保留期限的個人資料的執行細節；

(7) 制訂並實施有效措施以確保員工遵循上述第(4)及(6)項的政策及程序；及

(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。

40. 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

41. 《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)條就資訊系統遭勒索軟件攻擊向數碼港送達執行通知外，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。

設立個人資料私隱管理系統並委任保障資料主任

42. 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，並迅速應對任何資料外洩事故。機構亦應委任保障資料主任負責建立、設計及管理私隱管理系統，包括所有程序、培訓、監察／審核、記錄、評估及跟進，藉以監察《私隱條例》的遵從情況並向高級管理層匯報。

建立穩健的網絡保安框架

43. 隨著科技進步，機構對網絡技術的依賴程度越來越高。若網絡安全未得到充分保障，可能導致個人資料遭不當查閱甚至盜竊，進而對資料當事人以至機構本身造成無法估計的損失。因此，建立穩健的網絡保安框架對於防止資料外洩事故至關重要。就此，機構應了解系統當中所有可能被攻擊的伺服器或資料庫，以及它們可能遭到入侵的途徑，並在防範、偵測及應對網絡攻擊方面都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對資料保安所造成的損害。

適時對資訊系統進行風險評估及保安審計

44. 進行風險評估及保安審計對於防止資料外洩事故是不可或缺的。由於來自網絡的威脅不斷演變，機構必須持續評估其資訊安全狀態並識別潛在的風險。適時進行風險評估有助機構確定其資訊系統中的弱點及漏洞，並採取相應的措施予以修補。進行適時的保安審計則有助檢視機構制訂的資料保安政策、程序及措施是否妥善地被實行，從中識辨需要糾正或加強的地方。機構亦應在啟用新系統及新應用程式前，進行資料保安風險評估及保安審計，避免有關系統及應用程式成為資訊保安的新弱點。

建立重視資訊安全的企業文化

45. 資訊安全不僅涉及技術問題，更應是企業文化的核心。雖然技術措施是確保資訊安全的一重要部分，但更基本的是機構對保護所持有的各種資訊（包括個人資料）所持有的態度。事實上，資料當事人願意交出個人資料，是相信機構能妥善保護他們的資料。因此，機構妥善保障個人資料除了是法律責任之外，亦肩負道義上的責任。機構應透過價值的訂立，政策的推行及員工意識的培養建立一個重視資訊安全的企業文化，以確保機構由上至下都對資訊安全的重要性有正確的認知。

適時刪除個人資料

46. 機構不必要地或過長地保留個人資料，會增加資料保安方面的風險。因此，機構應按其職能活動及實際所需，制訂合適的資料保留政策以及相應措施，確保適時刪除已屆保留期限的個人資料，例如委派指定人員定期檢視資料保留政策落實的情況。