哈佛醫學院從端到雲

門鎖解決一成問題，記得鎖門需花九成功夫

已經步上雲端的哈佛醫學院，運用行動裝置提供更有效率的業務應用，還得防範內、外資安威脅。CIO 心得是，人與管理問題勝於一切。

文 | 吳依恂

哈佛大學是位於美國麻薩諸塞州劍橋的私立大學，亦為常春藤名校的成員之一，其醫學院 (HMS, Harvard Medical School) 亦在全美排名第一，可以說是公認相當優異的學院。該院的資訊長 John D. Halamka MD 提到，該校有 18,000 台電腦，6,000 台伺服器，3,000 名醫生和 300 萬筆病人的電子醫療記錄，因此他們經手處理的流量很大，皆是 Petabyte 級的巨量運算資料。

美國每年在醫療保健上的花費相當於四倍日本公民花費的金額，但卻還是有 4,000 萬人沒有醫療保險，但麻州卻是少數幾個 100% 公民都享有醫療保險的州，而有將近半數的醫生都採用電子病歷 (EMR, Electronic medical record) 來記錄（美國全國的平均數據是

20%），但越多的電子病歷當然也會有越高的風險。

維持巨量運算環境並不容易，再加上近年來行動裝置的盛行，哈佛醫學院如何一方面運用行動裝置提供更有效率的業務應用，一方面處理資安事件的威脅。先從三個真實的慘痛經驗談起。

疑似資料外洩事件

去年，HMS 發生了三件疑似資料外洩的事件。按照美國聯邦法的要求是，如果有超過五百筆病人的姓名被洩漏，則必須要盡可能的透過媒體，像是紐約時報或電視台等等，必須通知每個病人。Halamka 相當為難的說，這對 CIO 來說，真是一個極大的挑戰。不僅

真實慘痛經驗

1. 筆記型電腦被竊

HMS 打算建置一個私有雲，而在這個過程中，必須要將電子醫療記錄從舊系統轉換到新系統，他們也因此成立了一個專業團隊。這些電子醫療記錄包含了病人的資料，包括姓名、出生年月日、住址、社會安全號碼等。其中的一個技術專家，將一些 log 資料放在個人筆記型電腦裡，鎖在車上開回家，過了一晚，卻發現車窗被打破，筆電被竊，於是 504 筆病人的資料就這樣不翼而飛。把資料複製到自己的筆電上帶回家已經違反內部政策，這並非技術問題，而是人的問題。

2. USB 隨身裝置管理

哈佛醫學院主要的教學醫院－貝斯以色列女執事醫療中心 (BIDMC, Beth Israel Deaconess Medical Center) 為一國際知名醫療中心，年營業額可達百億美元，每年為超過 80 萬名的病患提供醫療服務，總共約有六千名職員。團隊當中，有一名藥劑師的主要工作，是分析醫療的抗生素施放量是否適當，於是他下載了病人的姓名、出生日期、診斷、藥品，到一個 USB 隨身碟裝置，Halamka 提到，該名藥劑師聲稱是要為自己的分析儲存副本備份。而這名藥劑師，隨後離開 BIDMC 前往加州洛杉磯，那裡並不似麻薩諸塞州的法律－所有處理醫療中心的筆電都必須全硬碟加密，於是在這名藥劑師將資料存到位於加州的筆電上之後。一天過去，筆電被偷了，2,000 筆病歷資料就這樣消失了，又過了一天筆電又被發現了，但裡頭的資料早已被清空。

3. 委外管理

這起事件發生在放射線工作站的單位。如同一般的醫院一樣，HMS 也採購設備，不過是由放射線工作站單位採購，並非由資訊部門直接購買，而作業系統內嵌在器材裡，於是設備商負責服務。問題就發生在於，負責服務的設備商，關閉了防毒軟體、更改了防火牆設定以便於連網。但不幸的是，該裝置中了病毒，造成了資料外洩的疑慮，而又根據法律，HMS 得通知所有在那台裝置上可以查得到資料的病人，Halamka 說，事件波及約有 2,000 人，而身為一個 CIO，他又得去向政府、媒體解釋，為什麼那些設備廠商可以關閉病毒軟體。

有違反相關醫療法律之虞，按照規定，每年醫療資訊的外洩事件的處理費用也極其昂貴，包括通知可能被資料外洩的當事人、購買他們的信用監控服務、通知聯邦政府、媒體等處理費用，光是「可能」外洩，計算起來，每筆資料的後續處理費用就要 282 美金。

從上述的例子我們可以看出，這些都不是技術性的問題，是人、是政策問題，Halamka 認為，好的資安防護應該是多層防禦。

▲ Jonh Haalamka 於趨勢 Direction 2011 活動發表 "The Security Journey of a Healthcare CIO：From Devices to the Cloud" 演說。圖片來源：趨勢科技提供。

針對醫療資訊的防護需求

從醫生的觀點來看，當然希望可以存取越多的醫療資料，以作為病人的照顧參考，或是研究，但從資安人員的觀點來看則希望能夠存取的人越少越好，應該如何在這之中取得平衡？ CIO 要求的是可用性，資安人員希望資料可以被控制，政府要求醫療資訊的保密性，合作夥伴們則要求資訊的準確性，確保不會被駭客竄改。

而為了達到諸多目的，HMS 採取了各種軟、硬體、政策擬定與教育訓練。在一些 IT 硬體架構上，HMS 採用了防火牆、IPS、WAF 等來進行網路防禦、偵測流量異常，軟體方面也有一些主動和被動的控制措施，包括最基本的防毒軟體、版本更新、監控、變更管理等。例如當有人同時，從不同的地點登入系統，就可以知道這不太尋常。因此必須掌握人們何時？從哪裡登入？登入頻率等。單單為了防護 300 萬筆病人的電子醫療記錄，Halamka 表示，HMS 一年就花了 100 萬美金來防範這些已知的病毒、駭客、惡意程式等。

政策層面：教育訓練、權限管理

根據 HMS 的預估，每年都有將近 6 成的醫學院學生，在網路上不當的揭露資訊。而他們除了學生之外，也有上千名醫生必須要管理，user 族群相當複雜。Halamka 說他們的用戶使用通訊狀況很複雜，但卻從沒想過安全問題。他們覺得走進咖啡店就可以連上網路很方便，卻沒有想到在外隨意使用無線網路有很多風險。於是資訊團

隊花時間教育這些醫生使用者，關於基礎的網路架構，如何分隔開公、私用途的信件、裝置等，如果在家連上網，必須使用特定的加密通道來存取資料。

此外，還要徹底進行稽核。這是一件相當困難的事情，Halamka 說，你很難透過稽核去規範哪個醫生可以去看哪個病人的資料。今天一個人突然被送進急診室來，哪個醫生可以看他的病例？你很難去預測誰會突然變成誰的病人。所以醫生可以看任何的病歷，但他們將會去稽核每件事情。

技術層面：透過工具、流程控管、加密

“Change is your enemy.” John Halamka 說。在行動上網的年代，每個人都想要用自己的裝置連上網，各式各樣的裝置和作業系統，iPad、iPhone、Android，每天都有許多軟、硬體在更新，但越多的改變就越可能出現漏洞，因為你不知道在更新之後，還有多少未被揭露的漏洞會出現，所以他認為必須控制所有的變更。

每週，HMS 的伺服器、網路、資安、桌上電腦等各團隊，都會進行版本變更的會議，透過一些文件的審核、程序等來允許各種變更，減少潛在的資安威脅。每晚，都必須檢查將近一萬五、六千台的電腦是否更新防毒軟體到最新版本，檢查 Log 是否有異常。例如說一個平常看 50 個病人的醫生，突然看了 100 個病人的病例資料，或是一個病人的資料一天之內被檢視了太多次，又或是在機敏資料的部分出現不正常的瀏覽流量，或是有人突然使用平常不用的應用程式等，透過這些例行檢視的步驟來降低威脅，而這是非常困難的，也都是 CIO 所要面臨到的挑戰。

並且，根據麻州法律，所有在行動裝置上流通的醫療資料，都必須經過加密。

行動裝置帶來的挑戰

HMS 共有三個資料中心，除了一個主要的資料中心以外，距離五英里遠以外還有一個災難備援資料中心，以及一個私有雲提供 2,000 名醫生使用。醫生們雖然是醫學方面的專家，卻不擅於管理伺服器，因此這個內部的私有雲是一個儲存資料的安全好地方。身為 CIO，他面臨到的新挑戰是，這些醫生大多是行動工作者，他們會從家裡、醫院、診所、護理站等不同的地方存取這些醫療資料，因此資安人員必須要掌控醫生可以從哪邊連上系統？使用何種裝置？ Halamka 開玩笑的說，最慘的是，iPad 已經變成最受醫生歡迎的行動裝置，因此他沒辦法說不，還必須讓他們一邊存取機敏資料，一邊玩 Angry bird ！

哈佛醫學院有 18,000 台電腦，6,000 台伺服器，3,000 名醫生和 300 萬筆病人的電子醫療記錄，因此他們經手處理的流量很大，皆是 Petabyte 級的巨量運算資料。

除了上述的一些控管措施，他也採取了角色的權限控管，醫生可以看到最機敏的資料，但其他的業務工作人員、專業研究員，僅能基於角色，獲得最少需求的資訊。

5 年前，人們攻擊哈佛只為了出名、讓人印象深刻。現在，則是為了利益，攻擊醫院和大學，不只是為了榮耀更能夠獲利。6 分美金，你可以從網路上跟犯罪集團買到信用卡號，1 塊錢美金就可以買到整個身分資料，像是社會安全號碼、駕照、護照資料等，10 塊美金買到銀行帳號，而且如果偷到智慧型手機，販售硬體至少得到 30 塊美金，而且販售當中的個人資訊，可能還比手機更值錢。這就是為什麼 HMS 必須要時時刻刻，一星期七天，一天 24 小時，每分每秒的進行安全監控、稽核、教育訓練使用者等。

Halamka 以他在哈佛醫學院的多年資安經驗來看，有九成問題都在於人的部分，如教育訓練、政策擬定、流程控管，卻只有一成是技術性的問題。他舉例，將門鎖上只是佔了 10%，但是記得把門鎖上、檢查門是否關上、確保其他人不會把門打開、管理鑰匙等，卻必須花 90% 的功夫。當 Hacking 已經從一件很酷的事情，變成一個犯罪集團的營利行為，這已經可以被稱之為戰爭了。在行動裝置盛行的現今，他認為資安只會面臨到越來越多的挑戰。