凡走過必留下痕跡
—談資訊系統的權限管理與稽核

※本文摘錄自本文摘錄於法務部清流月刊(作者：魯晏汝)

100 年 9 月時，某法院的法官被爆出利用職務之便違規查詢非辦案資料，該法官以其帳號登入法官查詢系統，對相親的對象進行身家調查，兩年來查詢筆數竟達八十幾筆；此外，也透過檢察官的辦案系統不當查詢將近五十筆的資料，其中還包括對院內有好感的女法官、女職員，她們的身家背景也一手掌握。

除了上述案例，在其他單位亦或是企業當中，也會有某些職務之性質是擁有查詢他人個人資料的權限，例如銀行行員因職務之需可查詢客戶的個資、信用紀錄，或與銀行往來的相關紀錄；企業單位部門主管可以查詢所屬員工的薪資及其他人事資料等等。因此，該如何因職務性質設定相對應的權限並進行及時的控管，便是件重要的事。

先從系統的權限談起。在設定系統權限時，常見的有依照使用者來做權限的區分，以及依職務/職位來做權限的區分兩種方式：

一、使用者區分：

舉醫院為例，如依使用者做區分，可概略將使用權限分成病人、掛號櫃台、醫生、後勤部門等。病人用自己的識別帳號（身分證字號或病歷號碼）登入系統後，僅能查詢到和自己有關的看診紀錄，並不能看到其他人的看診紀錄或是病歷資料；掛號櫃台人員使用自己的帳號登入後，也僅能看到掛號需要用到的基本資料，並不會因為他是醫院裡的人員就能隨意查詢病歷資料或醫院的人事及採購資料。

二、依職務/職位區分：

以醫生來說，可以依職務做區分，例如主治醫生、住院醫生及各科醫生，應該都僅能就自己負責的範圍內開放相關的系統權限；後勤部門的部分，例如財務、採購、人事部門的權限，也應依職務做區分，只能開放自己業務範圍內的使用權限，就像醫生使用自己的帳號登入後並不能查閱人事部門的院內人事資料，採購部門登入後也不能查閱病人的病歷及看診資料等等。

除了前面提到的依據使用者或職務/職位的權限做系統設定外，如果是像上述案例中提到的法官，因為本身職務性質的關係，其擁有的權限可用範圍就是可以查詢每個人的個資及其他相關資料，那該如何區別及控管查詢是否為工作中的正當使用，還是為非公務之濫用呢？

最重要的還是要有內部稽核的機制來做控管。當我們在**系統做任何操作動作時，系統裡都會留有存取紀錄（log），內部稽核單位應定期查核這些 log 紀錄，確認是否有異常之登入、查詢、讀取、新增、修改、刪除等存取操作**。如同上述案例，一般來說一個法官正常範圍內平均一個月會查詢兩三筆，但是案例裡這位法官登入的頻率是其他人的三倍之多，兩年下來重覆查詢了十多人，查詢筆數也高達八十多筆，像這種系統的登入及存取操作紀錄都應該定期被檢核，**如有異常的問題也可及時被發現**。

當然，我們都知道使用權限的控管和定期稽核的重要性，但是卻往往忽略很多小細節，例如：怕忘記密碼而隨手寫下自己的帳號密碼、將帳號密碼借給他人使用、共用密碼等等，這些都要盡量避免，因為這些行為都足以讓有心人士透過我們的帳號密碼從事不法的行為。此外，密碼也應該定

期更改，且新的密碼不宜與前幾次的密碼相同或有高度的重覆性，例如前一次的密碼為 Mary1234，新的密碼就應避免再次使用 Mary 或是 1234 等。另外，**不要使用自動登入及記住密碼的功能，因為這些功能都會將使用者的帳號密碼紀錄下來，很容易被有心人士利用**。關於密碼的選擇也應該避免使用全部數字、連續的字母或連號的數字、懶人密碼、出生日期、手機號碼、英文名字、字典裡的單字等容易被人猜出來的密碼，以及要盡量避免使用 1 開頭的數字或是 a 開頭的字母為密碼，因為在常見的暴力攻擊手法（Brute-force Attack）裡，都是從 1 開頭的數字或是 a 開頭的字母開始排列組合的。

最適合的密碼組合建議最少選用 8 個字以上，且含英文單字大小寫、數字或符號的穿插組合，例如「Happy+5372」可以變成「H5a3p7p2y」，或是在鍵盤上的連續位置按鍵「Vfr$%tgB」；另外也可以中文輸入法的按鍵作為密碼，例如「我的電腦」可以變成「ji32k72u04sl3」或是「ji#2k&2u0$sl#」（注音輸入法）等；還可以使用單字或是句子的第一個字縮寫做為密碼，例如「Never put off till tomorrow what you can do today」可以縮寫成「Npottwycdt」。這些組合都可避免密碼輕易地被測試出來。

凡走過必留下痕跡，在系統裡每一位使用者都應該擁有一組個人的使用者帳號做為唯一的識別碼，此使用者帳號即代表使用者在系統上的身分。每位使用者透過此帳號登入後在系統上的操作行為也應被存取紀錄下來，除了做定期的內部稽核外，如發生資安事件也可以依此紀錄來追究相關責任。