ISO/IEC 27001資訊安全管理系統認證

協助企業提升資訊保安

近年時有企業外洩客戶或公司資料。有見及此，部分公司着手建立及執行有效的資訊安全管理體系(Information Security Management System，簡稱ISMS)，並且透過申請ISO/IEC 27001資訊安全管理系統認證，以助確保資訊資產獲得充分保護。究竟ISMS涉及哪些業務層面？本地中小企應如何正視資訊保安的問題？

資訊安全管理體系（ISMS）是為了確保資訊獲得恰當處理和保護而設計。然而，由於資訊可以透過不同的形式存在，例如電腦檔案及所有實體文件檔案，包括影像、聲音等的資料，因此要妥善地安全管理資訊，往往比想像中困難。

本地企業應防患未然

香港品質保證局副主席何志誠解釋，一套良好的資訊安全管理體系，有助企業從多方面建立、執行、運作、監察、覆核、維護及改良資訊安全管理，當中以國際標準化組織（ISO）發布的 ISMS認證標準ISO/IEC 27001，在國際上較具知名度和認受性。何先生指出，此系統為資訊安全管理提供一套全面的框架，機構如符合ISO/IEC 27001標準的要求，便可申請由獨立第三方審核而發出ISO/IEC 27001認證，確認機構的ISMS已達國際標準，而成功獲取ISO/IEC 27001認證的機構可向外界展示其資訊資產已受到妥善管理，減低資訊保安風險，從而為業務夥伴及客戶帶來信心。

香港品質保證局副主席何志誠說，及早採取適當的資訊保安預防措施，有助企業避免聲譽或財務上的損失。

根據2015年度ISO管理體系認證證書調查報告的統計資料，ISO/IEC 27001自從第一版於2005年推出，並於同年引入香港以來，至今在本地共發出了141張證書。何志誠坦言，數字反映本地企業及機構可能基於不同原因，忽略加強資訊保安的重要性。他建議本地企業盡早推行系統化的資訊管理，避免因資料外洩而造成聲譽或財務上的損失：「資訊外洩小則導致客戶取消訂單，損害其市場地位及競爭優勢，嚴重者則可能須要面對法律訴訟，影響企業的長遠發展及因賠償而影響財政。」

中小企別低估對業務影響

對中小企而言，由於資金和人手的限制，資訊保安往往未必是老闆首要考慮投放資源的一環，但隨著市場環境的轉變，透過手機應用程式和社交媒體進行市場推廣及透過USB記憶棒或雲端服務儲存資料等運作模式日漸普及，日常業務中須要接觸和處理客戶資訊的渠道和機會愈來愈多，變相增加了企業出現資料外洩的風險。

香港中小型企業總商會常務副會長楊全盛指出，一般中小企老闆或因對IT欠缺足夠認識而低估了資訊外洩對公司的影響。不少中小企的老闆會將資訊保安事宜全權交由電腦部同事自行處理，而管理層則甚少參與其中；而部分中小企更以為投放了額外開支購買電腦保安軟件及硬件，便等同於做足了預防措施，但其實這些做法未必能全面保障公司的資訊。

他解釋：「一套完善的ISMS必須由企業內部全員作出配合，尤其是管理層的深度參與更為重要。若果管理層只依靠電腦部門主管去實施ISMS，而日後卻未有持續監察和改良系統，最終難免事倍功半。因此，管理層同樣須要積極參與並在政策上作出配合，帶領員工深入了解資訊安全風險對機構的影響和嚴重性，同時制訂日常工作規範及程序，提高員工的意識和警覺，方能全面提升資訊保安。」

香港中小型企業總商會常務副會長楊全盛表示，中小企在申請ISO/IEC 27001認證前可考慮本地認證業界為企業提供的支援服務。

他建議中小企在申請ISO/IEC 27001認證前，不妨考慮本地認證業界為企業提供的支援服務，例如參加培訓課程和研討會等：「畢竟中小企面對的資訊保安問題一般都大同小異，與其在毫無概念的情況下自行摸索，倒不如在專家指導下有系統地審視業務流程，更快找出容易出現資訊保安漏洞的地方從而對症下藥，省卻時間即等同節省開支。事實上，中小企架構相對簡單，實施ISMS更為容易。就長遠回報而言，中小企投放在ISMS的資源實為投資而非支出，提升資訊保安能對企業的未來發展帶來顯著裨益。」

工作坊分享用家心得

為了加強本地企業對資訊保安的認識以及推廣取得第三方ISO/IEC 27001認證的好處，香港檢測和認證局聯同香港認可處於2015年6月和2016年10月共舉辦了2場ISO / IEC 27001資訊安全管理體系工作坊，邀請了專家及已獲取認證的用家，講解如何合規地應用ISO/IEC 27001及分享申請認證時須注意的事項及事前的準備工夫，務求加強業界對於ISO/IEC 27001的認識，繼而了解獲得ISO/IEC 27001認證如何有助企業提升資訊保安。工作坊部分內容現時已上載於香港檢測和認證局網頁，供大家參考(www.hkctc.gov.hk/tc/work_seminars.html)。


香港檢測和認證局及香港認可處早前合辦ISO/IEC 27001資訊安全管理體系工作坊，加強業界對於ISO/IEC 27001的認識。

（資料由客戶提供）