從 ISO 9001:2015 看遠東商銀駭客入侵 — 超越驗證，才能創造價值！

工研院量測中心 ISO 9001 特約講師樊國紀

日前遠東商銀遭到駭客入侵，傳出駭客利用 SWIFT 交易前後兩波盜走 6000 萬美元，遠銀在 2017 年 10 月 06 日發佈重大訊息澄清，在積極追回匯款後，損失可望小於 50 萬美元，或完全追回款項。

對於遠銀遭駭被盜走新台幣 18 億元，2017 年 10 月 08 日，中國時報王莫昀小姐在「資安 5 缺‧駭客不上門才怪」的新聞評論中，指出國銀資安，有 5 大罩門亟待改善，分別是主事者心態不夠積極，技術不夠、管理不佳，缺乏人才，及資安主管層級太低。

王莫昀說令外界詫異台灣金融資安防護網竟如此薄弱，屢屢出包。冰凍三尺非一日之寒，問題癥結出在心態，面對資安，國銀多僅要求達到金管會的規定就好，反觀駭客卻不斷力圖技術精進，藉以四處攻城略地，為此，在這場資安競賽中，國銀不思改進，就只能祈禱駭客千萬別找上門！

其實國內很多銀行都有通過 ISO 27001 資訊安全管理系統驗證，那為什麼還會有主事者心態不夠積極，技術不夠、管理不佳，缺乏人才，及資安主管層級太低這些管理上的問題，是標準沒有用，還是驗證不可靠，這的確很值得大家深思。

ISO 27001 與 ISO 9001 一樣都是以 PDCA 管理循環為基礎之管理系統標準，只是一個是規範資訊安全管理，一個是要求品質管理。目前依照 ISO 9001, ISO 27001 這些管理系統標準，建立系統化管理制度，並申請驗證，是全球的趨勢。但是系統符合標準，並不代表績效卓越，同時驗證浮濫、形式化與表面化的批評也時有所聞。

我從民國 80 年開始接觸與參與 ISO Guide 25, ISO 17025 與 ISO 9001 這些管理系統的認證與驗證工作，這二十幾年的工作經驗讓我知道其實大部分的企業或組織，都是抱著及格就好的心態與做法，只知道要通過驗證，卻沒有掌握到管理的精義與訣竅。所以國內雖然引進了歐美的理論與標準，但能融會貫通的，真的是不多，所以就常會碰到主事者只知道不要有不符合事項，自我要求太低，不夠積極，負責人員位階偏低與權限太小，技術與管理不到位這些情況。

所以如果希望能發揮管理系統之效果，最重要的就是要先調整這種及格就好的心態，因為驗證不應該是推動管理的最終目標，確保產品品質與資訊安全，創造營收與利潤，才是管理的目標。所以根據 ISO 9001 或 ISO 27001 建立制度時，真正要優先考慮是要如何有效管理。就像考及格不應該是學英語會話的最終目的，

能夠用英語流暢的表達與溝通，才應該是學英語會話的目的。

筆者在 98 年 11 月 27 日，於 2009 年管理系統與產品認驗證論文發表會中，發表如何提昇管理系統驗證之價值一文時，即指出管理系統驗證基本上只是符合性驗證，而 ISO 9001 這些共通性管理系統標準(Generic management system standards) 只規定要執行那些工作，但對於要如何作則要求不多，因此雖然及格就能通過驗證，但如果只是抱著及格就好的心態，那符合標準就只是表示該作的事情有作，但並不代表所用的方法，能使工作產出達到一定的績效水準。

因為驗證是外在的要求，對於這種外在的要求，就像孔子所說：「道之以政，齊之以刑，民免而無恥。道之以德，齊之以禮，有恥且格。」大家通常只是奉命行事，被動的符合標準，所以只靠外在要求，不足以激發團隊的熱情，去持續學習與應用更好與更有效的方法，因為如果只求通過驗證，不想用心努力，自然就會只想用簡單的方法，所以當然也就不容易看到效果。

就像學英語會話一樣，除非內心真的有興趣學，否則英語會話及格，碰到國外客戶，卻不一定能夠向用英語流利表達。因此很明顯的，及格並不代表擁有優異的專業能力，如果想要擁有出眾的專業能力，及格之後還要持續的學習與努力，所以通過理系統驗證之後，也要不斷的改進與突破，才能期望看到傑出的績效。

因此對企業或組織來說，除了依照管理系統標準建立制度，更重要的是要由領導者以身作則，不是只要及格通過驗證，而是要有效運用標準，追求卓越，然後發揮風行草偃的功效，經由領導與激勵，塑造真正的品質與資安文化，培養自動自發、積極學習、自律有恆與團隊合作的工作態度與專業精神，創造一個內在激勵所驅使的環境，帶領團隊持續的學習、改善與創新。

因為只有經由內在激勵，激發員工的熱情、專注、潛能、衝勁、與使命感，促使工作同仁基於個人的價值與信念，而主動參與採取行動，運用正確有效的方法，執行各項工作，達成績效目標，並不斷的精益求精與創新突破，我們才能真正發揮管理系統的功效，創造管理系統驗證之價值。

作者簡介：

工研院量測中心 ISO 9001 與 ISO 17025 特約講師樊國紀

樊國紀為成大土木工程碩士，英國 IRCA 與德國 TRCert 認可 ISO 9001 主導稽核員，現為 TUV Rheinland 台灣分公司特約 ISO 9001 稽核員，曾任 TUV Rheinland 台灣分公司資深專案經理、ABB 台灣分公司品質經理、大陸工程公司品質部經理、工研院量測中心機械認證部經理，有 30 年實務經驗，熟悉國際標準 ISO 9001 與 ISO 17025 之理論與實務。