鼓勵資安防護成效並以獎勵取代懲罰，方能澈底提升整體資安防護能量。

資訊安全典範個案

◎盧玲朱

壹、研究目的

本次個案研究之目的在於透過政府機關的觀點，了解在社交工程演練過程中展現極卓越之政府機關，針對機關如何形成良好的資安環境與管理機制，來改變組織成員之認知與強化資安行爲，並發展歸納出落實資安管理之行爲模式。

本個案採取質性研究方法，以質性的程序進行研究上的分析，而非藉由統計的程序或其他量化的數據產出研究成果。質性研究方法之特點在於依據研究的對象，探討組織或個人在行爲方面的影響，能夠於個案設計的情境下，深入發掘其中的各種活動與過程。

貳、個案說明

個案研究對象爲執行資安管理制度成效良好之甲部會，藉由訪談甲部會與其遴選之六個所屬機關以了解政府機關執行社交工程演練之行爲模式。

甲部會爲全機關導入 ISMS 的政府機關，驗證範圍爲資訊處及部本部的所有局處。對於社交工程演練的表現，通常落於平均水準附近，演練情形處於平穩的狀態。

甲部會下轄三種類型的所屬機關，分別爲Ⅰ類型機關、Ⅱ類型機關及Ⅲ類型機關；各類型機關之業務屬性及特性皆有差異，因此於每類型機關中各遴選兩個所屬機關進行訪談研究。初步介紹六個(No.1～No.6)所屬機關背景說明（如表１）與三類類型機關綜合比較說明（如表２）：

表１ 六個所屬機關背景說明

三類型機關	代表機關	特色
I類型機關	No.1機關 No.2機關	主管重視資安工作 機關人員遵循性與配合度高 無資訊室與資訊人員 業務需使用資訊系統程度低 缺乏資訊預算編列
II類型機關	No.3機關 No.4機關	大量使用替代役及委外人員 業務需使用資訊系統程度高 機關規模較小
III類型機關	No.5機關 No.6機關	主管重視資安工作 人員自主性及獨立性高 設有資訊室及資訊人員 缺乏資訊預算編列

資料來源：本研究自行整理

表 2　三類型機關綜合比較表

比較項目	I類型機關	II類型機關	III類型機關
主管重視資安程度	高	高	高
機關規模*1	約80~300人	約40~60人	約120~400人
人員特性	遵從性高	一般	自主性高
使用資訊系統程度*2	低	高	高
委外人員及替代役人數	少數	約50~100人	少數
資訊預算編列	無	無	無
資訊室與資訊人員配置	無	無	約1~2人

*備註：

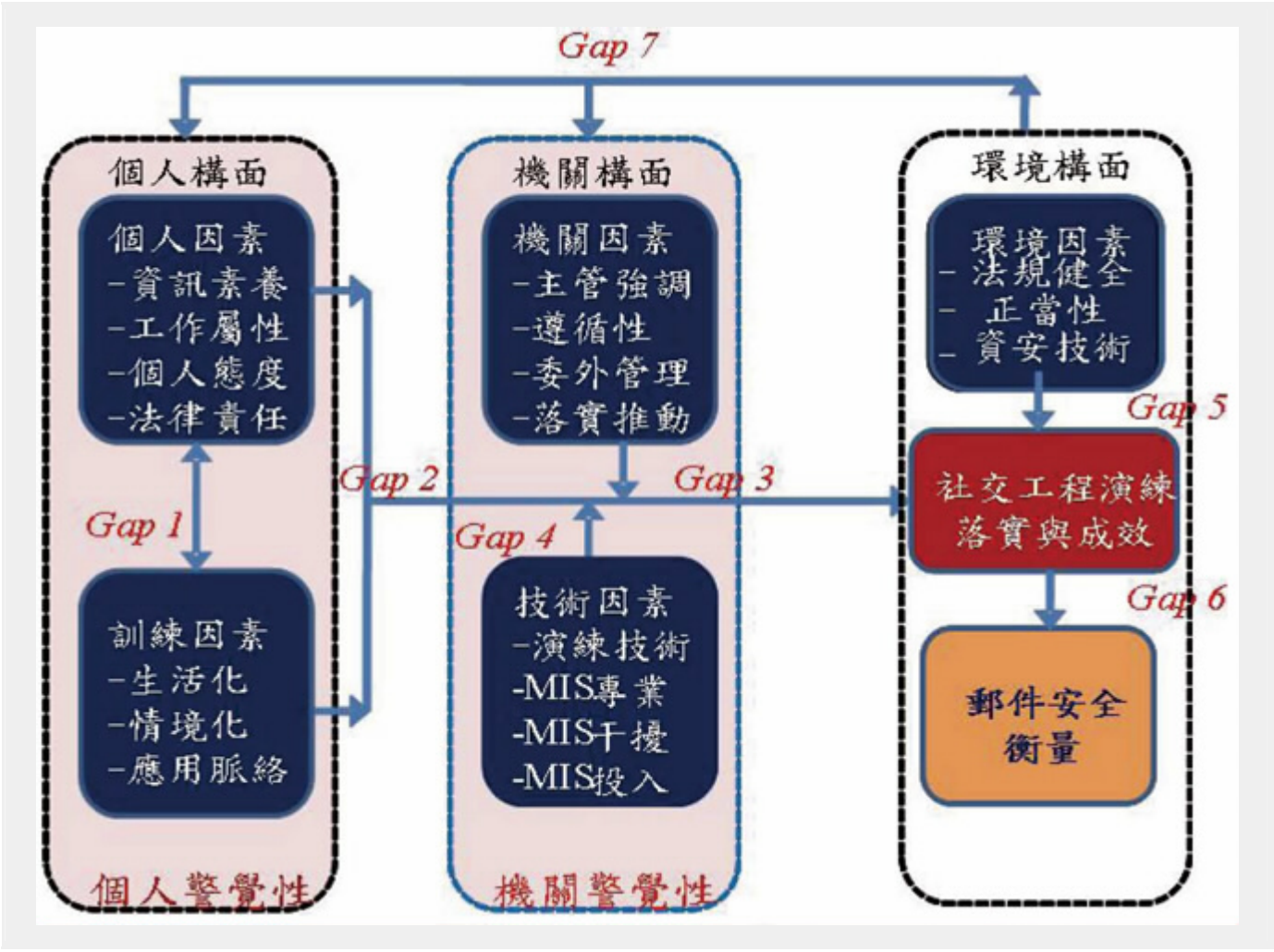
1.「機關規模」表示該機關正職人員數目，不包含委外人員及替代役。

2.「使用資訊系統程度」指該機關業務上需使用電腦協助處理之必要程度。

資料來源：本研究自行整理

參、研究分析成果

本研究依照所遴選之六個單位，針對其社交工程演練之行爲模式，進行深入訪談，並依照行爲模式之個人、機關及環境三大構面，分析本個案之行爲落差分析，歸納出以下七點落差(Gap)，詳見圖１。



資料來源：本研究自行整理。 圖 1　　社交工程落差分析

- Gap 1 教育訓練方式與教材內容未完全符合個人屬性與其工作屬性：目前資訊安全認知訓練採取的方式爲所有機關人員一起上課，並無針對人員的工作屬性來區隔訓練的內容。
- Gap 2 社交工程的成效不等同於個人在郵件安全的警覺性：個人警覺性是影響社交工程成效的重要因素，它僅能代表社交工程的部分成效，不代表著整體成效。
- Gap 3 機關因素不一定應對個人資安認知有正面影響：機關因素的影響不一定能有效提升個人的資安警覺，從而提升執行成效。在機關因素的影響當中，最重要的是機關主管對於資訊安全的重視與強調，若機關主管高度重視資訊安全，則課程訓練勢將安排較多，個人資安認知即相對提高；反之，則個人認知即降低。
- Gap 4 機關警覺性介入雖能美化演練數據，但對於個人警覺卻無實質提升：機關警覺性最重要的因素是 MIS（management information system）人員介入，MIS 人員（即資訊系統管理者）常於資安演練時求好心切，而使用各種方法影響機關的演練成績。
- Gap 5 不健全的資安環境阻礙社交工程的落實並降低成效：資安政策及執行事項欠缺完整法源支持，執行之資源與成果均有所限制。

- Gap 6 應加強社交工程的落實與電子郵件安全間的關聯性：機關常因爲重視演練成效，經常透過管道影響個人警覺，導致個人資安意識與警覺性無法於演練中衡量。
- Gap 7 不完善的資安環境無法有效提升個人與機關之警覺性：我國現行的資訊安全相關法規散見於各主管部會，缺乏資安專法的法源基礎，以致於個人與機關之警覺性無法有效提升。

肆、結論與建議

本個案之研究目的在於透過行爲面的研究以了解各政府機關落實資安管理工作的實務，然而本研究以質化方法作爲主要的研究策略，屬於初探型態研究，無法顧及所有的資安管理事項，故研究範圍限定以社交工程演練作爲主要的研究主軸，藉由理論研討及訪談分析，探索其推動資安管理之現象，從中建構理論模型並加以解釋。

根據本案之研究分析成果得知，個人與機關對資訊安全之重視，實能影響其資安防護表現，進而於內部建立更多的資安制度，俾能強化資安認知概念。資訊安全社交工程演練係爲了解個人及機關對於郵件安全意識而設計之活動，然而機關卻常因重視演練成效，而過度干擾整體演練過程，以致影響整體的演練成果。因而如何建立個人與機關之資安意識，鼓勵資安防護成效並以獎勵取代懲戒，方能澈底提升整體資安防護能量，否則以駭客日益精進的技術看來，資安防護甚難做到萬無一失。

由本案之研究了解，政府單位在推動資安工作時，應考量從整體環境面建立體制，從訂定資安法律及制度進而輔以各項政策及措施，並搭配各項檢查機制，以帶動機關與個人遵循相關規定，同時養成正確的資安習慣以期獲得良好的運作成效。因此，針對我國所推動的資安工作，提出以下四點建議事項：

一、 訂定資安專法，以提升資安工作推動之正當性：相較於其他先進國家而言，我國缺乏資訊安全的專法，以致於資安相關工作之推動缺乏足夠的正當性，影響資安工作的落實。因此，爲強化政府機關推動資安工作之正當性，長期而言，仍應訂立資安專法爲資安的推動建立法源依據。

二、 增加各機關之資訊與資安專職人員，以提升機關之資安應變能力：由於資訊人力的不足，導致常以其他部門的人員兼任，造成工作負擔過重及專業知識不足的問題，影響機關資安工作的落實。因此，爲加強政府各機關單位的資安應變能力，各機關單位至少應設置一位以上專職的資安與資訊人員，以提高其資安應變能力。

三、 推動客製化資安教材，以提升資安認知訓練的成效：從知識建構理論的觀點而言，知識的建立應搭配合適的情境脈絡，才能達到良好的成效。由於政府各機關人員對於資訊使用的情境各有不同，故應搭配不同的資安個案與教材來輔助訓練教學，方能達到教育訓練的預期績效。

四、 區隔電子郵件帳號使用性質，提高電子郵件使用之安全警覺：現行大部分機關人員使用電子郵件時，常將私人與公務的郵件使用同一帳號處理，較易降低對郵件使用的安全警覺性。因此，爲提高機關人員對於電子郵件使用之安全警覺，建議應區隔私人與公務間的電子郵件帳號，並針對公務電子郵件提供更嚴謹的使用機制（如提供電子簽章等），以提高機關人員處理公務電子郵件的安全警覺。

（作者現任國家資通安全會報技術服務中心正規劃師