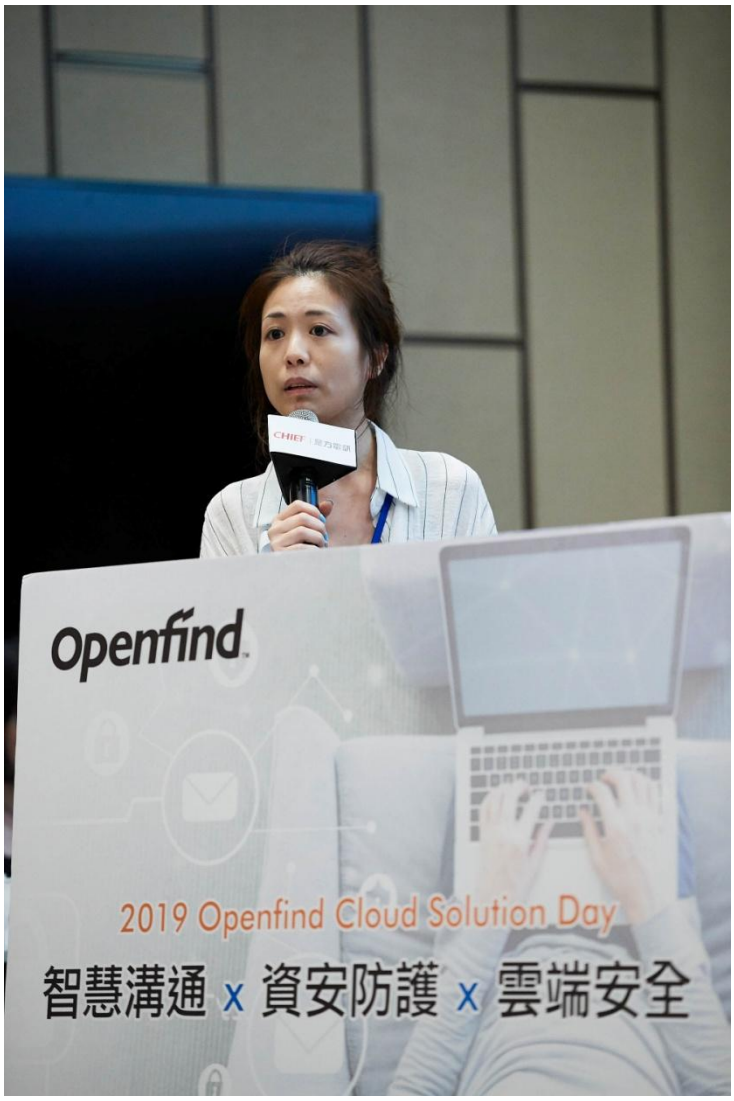
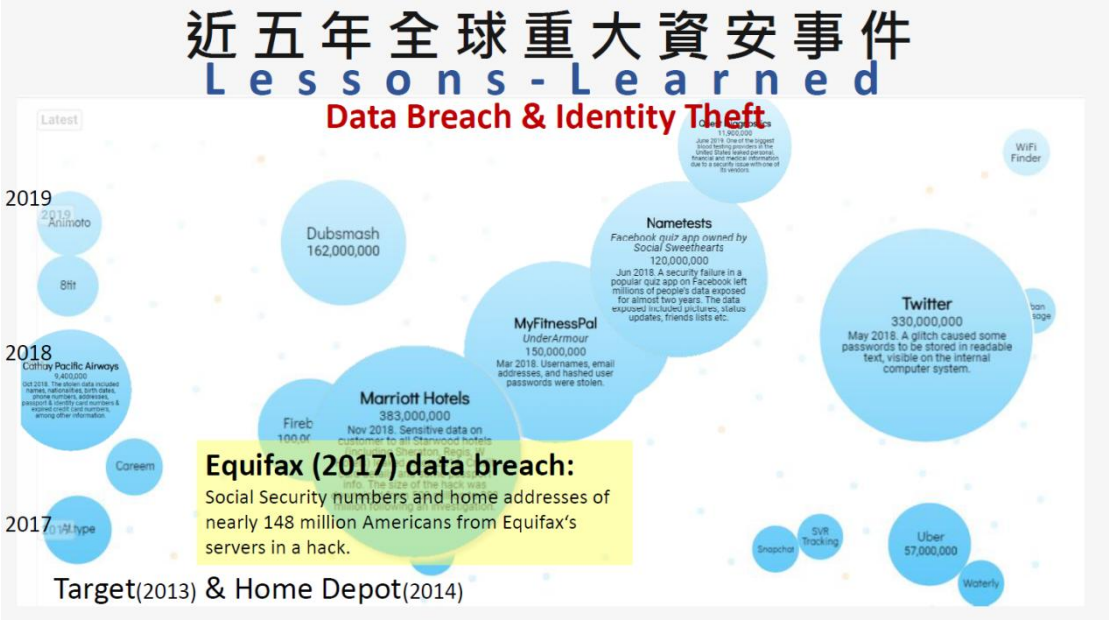
近在眼前 視而不見的頭號資安危機



(是方電訊 產品經理 陽琪)

檢視過去五年來全球發生的重大資安事件可發現許多知名企業均榜上有名，是方電訊產品經理楊琪列舉：無論是大規模的傳統產業，如跨國飯店集團萬豪、國泰航空，或是知名的原生數位企業，如推特 Twitter、優步 Uber、英領 LinkedIn 等，均在五年內發生過重大資安事件。



上述企業並非未建立資安防護，反而是投入可觀資安預算資源、人力編制落實防護，但為何仍然發生慘痛的資安事件？究其原因在於「資安破口」，雖然企業自身已完善資安防護，但與企業往來的上下游合作夥伴其規模有大有小，能投入資安防護的資源不同，對資安建置的態度亦不同。而企業與夥伴間有資訊往來，駭客與有心人士即從整體供應鏈的弱處下手，最終依然得逞而造成資安事件。

同樣的，凡中大規模以上的行動通訊營運商、雲端服務營運商，均已從底層開始要求與建立資安防護，駭客同樣不從有備之處進攻，而是從實際防禦、心理防禦均相對為弱的用戶端下手，特別是一些終端使用者樂於在網路上分享，或在社群上輕易加入好友，或對小型、不明網站輕易選擇以社群帳號連結登入等，如此有心者即有機會收集到足夠的所需資訊進而加以運用。

由於駭客已收集充分個資，而在國外要更換手機號碼、SIM 卡等相對容易，不似我國需出示雙證件，駭客因而取代本尊要求更替手機號碼，如此即便有手機簡訊驗證程序駭客也能正確回應，駭客被認可為真身後開始對各服務機構要求個資變更，反而使原用戶成為非法者，權益因而受侵害。歸結上述癥結仍在於終端使用者薄弱的防備，使駭客有機可趁。

針對終端用戶的資安防禦楊琪建議導入雙因子、多因子認證，即除了圖形鎖、密碼鎖之外可再加增指紋辨識、人臉辨識，提高整體驗證難度。此外是方電訊也建立、營運應用雲平台 CHIEF App Cloud，平台上的 iDenPass 即支援雙因子認證機制。

而是方電訊與網擎資訊的合作，由網擎提供信件、檔案層級的防護，是方則專注於身份辨識、登入驗證層面的防護，即建立起整體防禦中的第一道防線。

終端使用者一旦導入是方應用雲 CHIEF App Cloud 的 iDenPass 方案，即可保護個人機敏（機密、敏感）資訊，避免遭受釣魚網站的社交工程攻擊，避免中間人攻擊，以及避免先進持續威脅等。

另外在系統層面採行的是金融銀行等級的加密，且合乎國際 Oath 協定。進一步的，iDenPass 方案也提供完整的驗證紀錄，便於企業落實稽核制度以及資安意外發生時可配合調閱、協助鑑識。此外方案採行動態金鑰管理系統，由伺服器端執行驗證，也同樣助於整體資安防護強度。

一旦落實多因子驗證，資安的短板（木桶原理 Cannikin Law）、破口即不再是終端使用者，整體防護強度提升，同時資安人員當重新檢視整體防禦，發現新的弱項、脆環，而後研擬補強防範策略進而行動。唯如此能使企業持續專注於業務創新與拓展。