

強化資訊安全的第一道 防線 - 資安意識

Cyber Security Awareness

2023年5月11日

報告人：陳志明



陳志明
副總經理
安永諮詢服務

Mobile +886 936 169 800
Tel +886 2 2757 8888 #67836
Email Jemmy.CM.Chen@tw.ey.com

背景介紹

學歷

- ▶ 中山大學 資訊管理研究所 碩士
- ▶ 中山大學 資訊管理學系 學士

專業資格:

- ▶ CISSP
- ▶ CISA
- ▶ ISO 27001 LA
- ▶ BS 10012 LA

相關工作經驗

- ▶ 具備金融、高科技、電信等產業商業及資訊流程的風險管理經驗，在資訊安全、機敏資料/個人資料/隱私權保護相關領域有超過15年的工作經驗
- ▶ 協助多家金控、銀行、保險及證券公司建構資訊安全風險管理架構，並取得資訊安全管理制度 (ISO 27001)及個人資料保護管理制度(PIMS)國際認證
- ▶ 協助多家半導體、資訊電子業公司執行資訊安全風險管理，資訊安全架構設計、資訊系統安全評估 (包含弱點掃描、滲透測試)，建置ISO 27001資訊安全管理制度，並取得國際認證
- ▶ 負責過20個以上資訊安全/機敏資料保護/個人資料保護專案，協助客戶建置資訊安全管理制度、個人資料保護管理制度，並取得國際認證
- ▶ 主要的客戶群包含半導體、資訊電子、電信、金控、銀行、證券與保險、汽車、零售等產業

專業能力

- ▶ 資訊安全風險管理制度建置
- ▶ 資訊安全架構設計與評估
- ▶ 資訊安全解決方案設計
- ▶ 機敏資料保護與管理
- ▶ 個人資料保護/隱私權管理
- ▶ 供應鏈風險管理評估
- ▶ 資訊科技環境控制諮詢
- ▶ 一般資訊循環及應用系統查核
- ▶ 資訊循環控制制度設計及覆核
- ▶ 資安/SOC確信

1

建立資安意識文化的 議題

什麼是資安意識？

意識 Awareness

知道和理解某事正在
發生或存在

培訓 Training

一種技能發展方法，
學習完成特定工作或
活動所需的技能

教育 Education

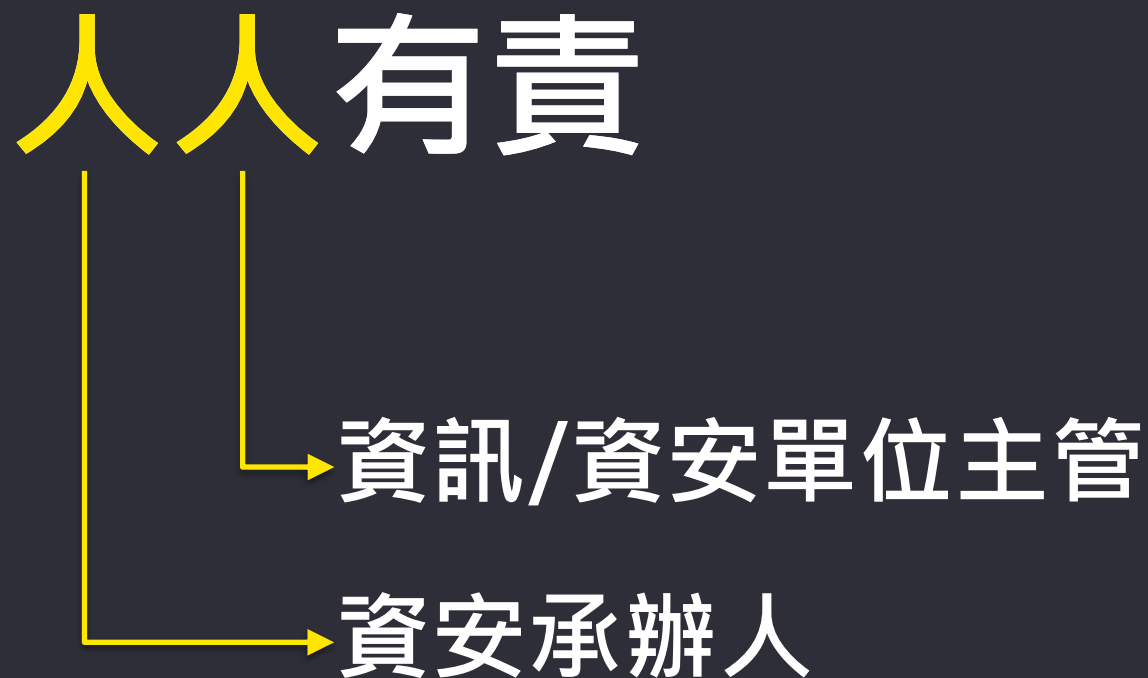
培養判斷力和推理能力；
教育是指獲得廣泛的知
識和技能

創造意識不是讓人害怕；而是關於授權並使人們採取行動，為他們提供正確的控制、良好的習慣和所需的工具。

身為一個專業的資訊/資安專家，你知道 ...

資訊安全

人人有責



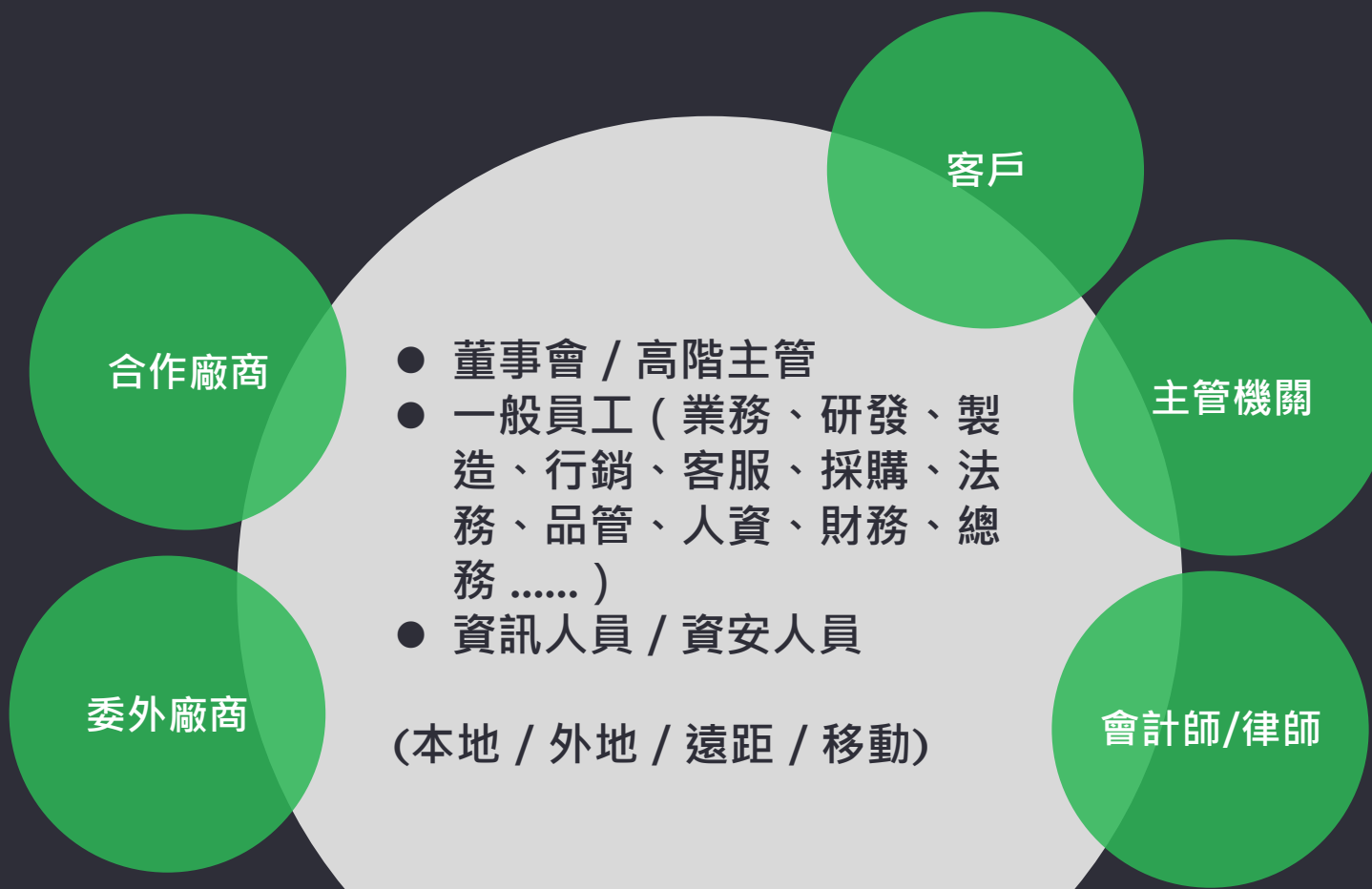
資訊/資安單位主管

The diagram consists of two vertical yellow lines descending from the characters '人人' in the title '人人有責'. From the right vertical line, an arrow points to the text '資訊/資安單位主管'. From the left vertical line, an arrow points to the text '資安承辦人'.

資安承辦人

身為一個專業的資訊/資安專家，你知道 ...

資訊安全 人人有責



「人」已成為全球網路攻擊者的主要攻擊媒介

“

「人」已成為全球網路攻擊者的主要攻擊媒介，
因此現在對組織構成最大風險的是人，而不是技術。

— *SANS 2022 安全意識報告*

SANS 2022 安全意識報告分析了來自世界各地的一千多名資安專業人員的數據，以確定組織如何管理其人為風險。

根據 FBI 發布的資料，自 2016 年至 2021 年，商業電子郵件詐騙(BEC攻擊, 社交工程)造成的損失
超過 430 億美元。

Verizon 的 2022 年資料洩露調查報告 (DBIR) 顯示，
82% 的資料洩露事件是
人為因素造成的。



- ▶ 資安意識月 (Cybersecurity Awareness Month) 由美國國家網路安全聯盟(NCA)、美國網路安全暨基礎設施安全局(CISA)發起，為每年10月舉辦，至今已邁入第19年。
- ▶ **每年強調不同的主題，提升大眾的資安意識。**

- ▶ 2022年特別呼籲的資安防護觀念為：
 1. 帳戶啟用多因子認證(Multi-Factor Authentication)
 2. 使用高強度密碼
 3. 對疑似釣魚詐騙、手法保持警覺性，並即時回報給相關單位
 4. 軟體更新至新版

我國政府也正視資安意識的重要性

法規名稱：資通安全管理法 **EN**

公布日期：民國 107 年 06 月 06 日

法規類別：行政 > 數位發展部 > 資通安全目

第 4 條 1 為提升資通安全，政府應提供資源，整合民間及產業力量 **提升全民資通安全意識，並推動下列事項：**

一、資通安全專業人才之培育。

二、資通安全科技之研發、整合、應用、產

三、資通安全產業之發展。

四、資通安全軟硬體技術規範、相關服務與

2 前項相關事項之推動，由主管機關以國家資

上市上櫃公司資通安全管控指引

第二十八條、 每年定期辦理電子郵件社交工程演練，並對誤開啟信件或連結之人員進行教育訓練，並留存相關紀錄。

法規名稱：金融機構辦理電腦系統資訊安全評估辦法

時間：中華民國107年3月22日

所有條文

編章節

條文檢索

歷史沿革

相關令函

相關判解

制定依據

附屬法規

🔍 條文關聯

🔄 回上一頁

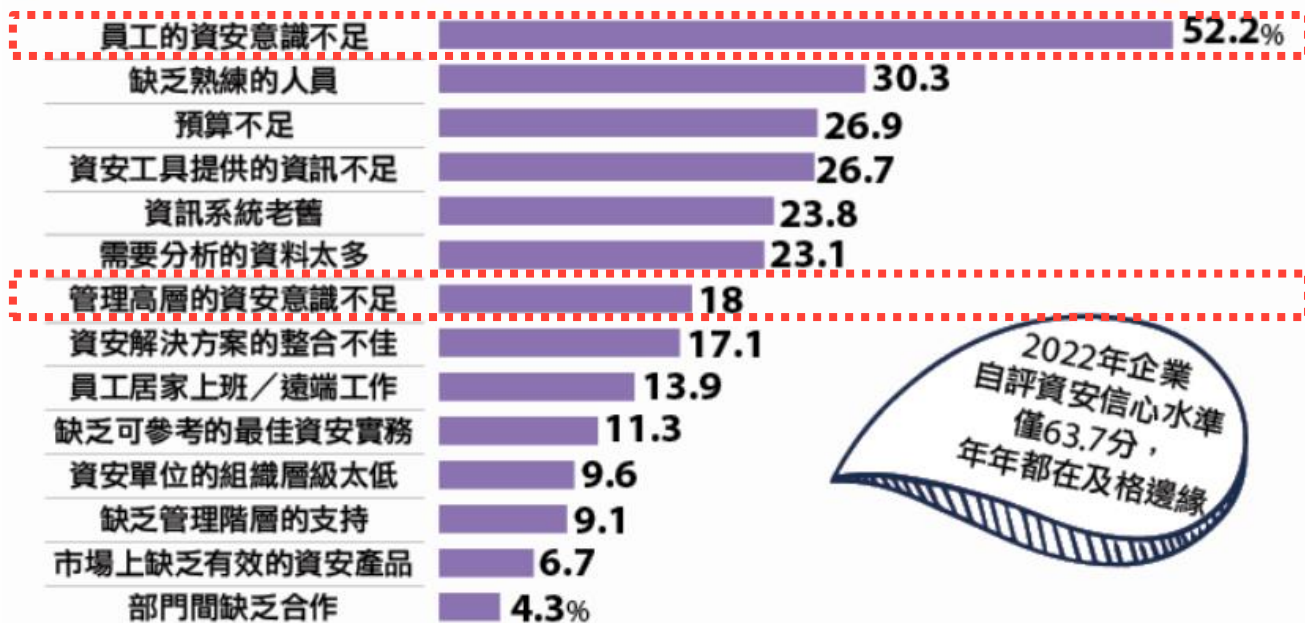
第六條社交工程演練

每年應至少一次針對使用電腦系統人員，於安全監控範圍內，寄發演練郵件，加強資通安全教育，以期防範惡意程式透過社交方式入侵。

台灣企業的資安意識夠嗎？

為何企業難以抵抗資安攻擊（資安弱點排名）

員工資安意識仍是主因，資安老手不足問題日益嚴重



說明：百分比為CISO自評遭遇該項弱點的企業比例

資料來源：2022 iThome CIO大調查，2022年8月

iThome

2022年企業
自評資安信心水準
僅63.7分，
年年都在及格邊緣

- 根據2022 臺灣企業資安曝險大調查，多數企業輕忽社群媒體所衍生的網路攻擊。
- 大部分企業都擁有社群媒體的專頁，且員工也非常容易於社群媒體上暴露自己的公司聯絡資訊，導致駭客發動魚叉式精準社交工程時，成功得手機率大增。
- 連續5年，**員工資安意識不足都名列第一**。這也可以說是臺灣大型企業業最大的資安弱點。

去年也沒有例外，高達52.2%企業在去年因此而擋不住資安攻擊。

大多數資安意識計畫並沒有完全達到其目標

意識計畫使資安團隊能夠透過改變人們對網路安全的看法，並幫助他們實踐安全行為來有效地管理他們的人為風險。

1

缺乏人們的
參與和積極性

意識計畫聚焦於公司政策，未能傳達安全行為(secure behavior)如何在個人層面上使人們受益的資訊。

2

意識被視為
“一次性”的練習

完成強制性e-learning創造了一個人們知道測驗答案的環境，但沒有採用或衡量安全行為。

3

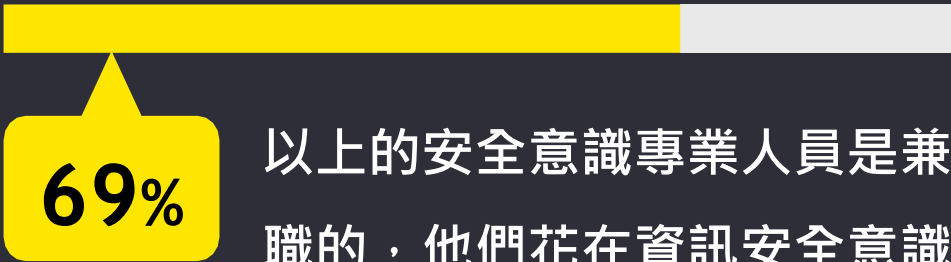
意識計畫沒有因應
組織的環境和風險
而調整

雖然有許多現成的意識解決方案可用，但組織通常不會投資於解決其特定業務環境和面臨的威脅的解決方案。

安全始於意識

在當今無邊界的工作場所，全面的安全性至關重要。

這種 360 度保護需要**教育和意識**來保護身份、資料和設備。



69%

以上的安全意識專業人員是兼職的，他們花在資訊安全意識上的時間不到一半。

全職定義為將 70% 或更多時間用於安全意識的人。

2

資安意識訓練的類型 與效益



建立有效的資安意識計畫

1. 認識風險

利用威脅情報和市場知識，研究適用於組織的威脅者和攻擊方法



3. 選擇目標受眾群體

對於每個已識別的風險，選擇合適的受眾。



4. 使用正確的溝通方式

分析現有的溝通管道和文化。



8. 選擇有意義的指標

選擇有意義的指標衡量安全實踐的嵌入並確定可能的改善計畫。



7. 使用遊戲化戰術

通過使用遊戲化技術和誘人的競爭，在意識倡議中引入多樣性。



6. 加強資訊與內容

加強主要內容以維持持續學習。



5. 發展引人入勝的內容

使資訊具有相關性、身臨其境、有趣和個性化。



2. 將人類風險與預期行為聯繫起來

確定常用技術和陷阱如何與人類行為相關聯，並了解為什麼目前沒有遵循該行為。



因材施教，設計符合不同目標群體的資安意識培訓計劃

人是任何公司資安戰略中最重要因素，投資意識計劃對幫助他們實現目標有很大的幫助。

Security Awareness Program

安全意識計劃的主要目標是確保將安全嵌入到組織中。為了達到預期目標，它應該無縫地將**安全目標與業務目標聯繫**起來。

意識計劃通常持續一年，旨在透過不同的解決方案並在最佳時機，向定義的**目標群體**展示相關主題。



所需時間

根據成熟度，安全意識計劃可以長達24個月的時間。



交付項目

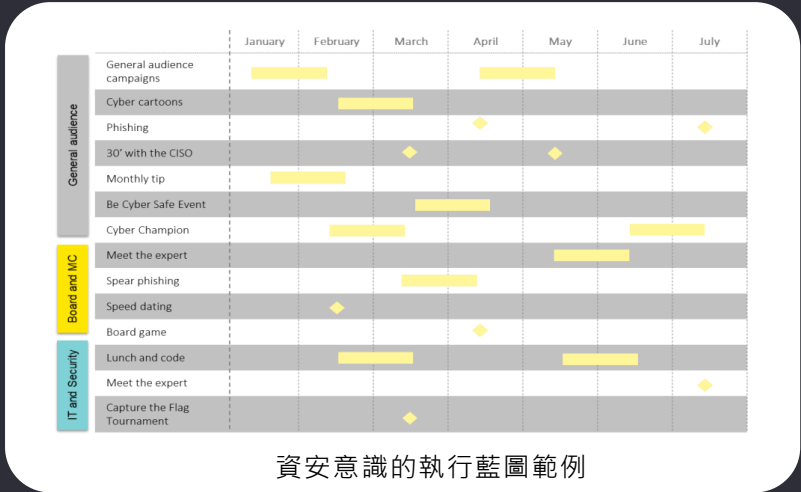
適合組織需求和預算的安全意識策略和計劃。
執行中的計畫支援。

主要效益

- 強調組織特定的風險和行為改變
- 整個組織內的方法結構化

成功因素

- 領導參與
- 長期的計劃
- 客製化培訓計劃 vs. one size fits all



資安意識的執行藍圖範例

常見的資安意識訓練方式



線上學習課程 (E-learning Modules)

E-learning sessions 透過幫助整個組織中達到統一的網路知識水平，來支持資安意識計劃。



E-learning Modules

內容根據培訓課程和清楚的學習目標設計，側重於組織特定的內容。可以開發該模組以合併(包含)視覺效果、練習、遊戲化選項和品牌元素。

E-learning 模組可以重複使用，並且可以隨著時間的推移，進一步調整以反映可能的流程、技術或網路環境變化。

主要效益

- 自學
- 隨時可用
- 即時 KPI
- 完全客製化的內容
- 有吸引力的視覺效果

主題類型範例

- 網路釣魚
- 遠程辦公
- 資料保護
- 實體安全
- 社交工程
- 網路應用程式的安全使用



所需時間

完成一堂e-learning模組需要20-60分鐘



建議對象

一般受眾皆可



執行方式

E-learning 模組，自選的知識驗證（最終測試）和指標。

該模組可以僅作為內容提供，也可以作為以最終可視化E-learning格式開發的內容提供。

高階主管訓練 (Executive Training)

主管培訓是針對高層領導的特定資訊安全主題培訓。

主管培訓著重於關鍵資安主題，以便更好地了解資訊安全以及應該從戰略上做什麼來定義、監控和報告風險偏好。

培訓主題涉及網路威脅形勢、合規性和監管要求、資安風險監督、資安管理和資安技術框架以及個人安全檢查表等要素。

Executive Training



所需時間

培訓課程深度根據需求而定，持續時間約為1至4小時，具體取決於現有的資安知識。



建議對象

董事會、最高管理層和高層主管

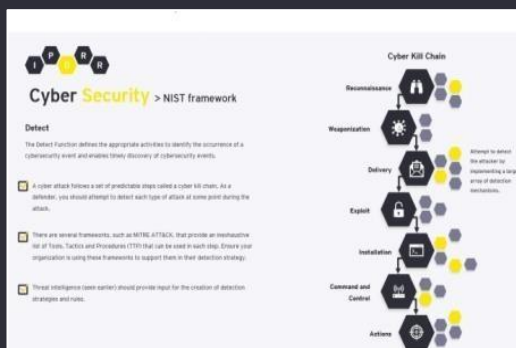


執行方式

由資深專家進行現場或遠端培訓課程，可以是個人的或以組的方式進行，實際上會根據需求而不同。

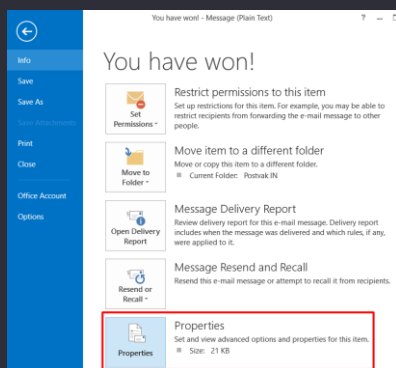
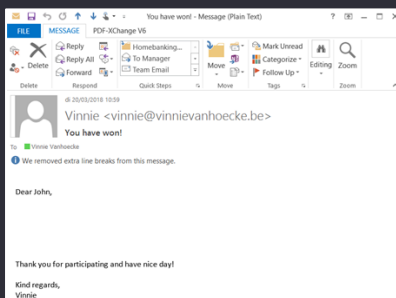
主要效益

- 客製化內容
- 跳脫技術細節
- 適應需求
- 開放式對話
- 分享市場地位和經驗提供有意義和具體的見解



釣魚攻擊 (Phishing Campaign)

網路釣魚活動是一種測試員工對欺詐性電子郵件的意識以及他們如何防禦的練習。它具體衡量組織對網路釣魚風險的準備情況。



Phishing Campaign

除了錯誤點擊可能造成的災難性後果（金錢、智慧財產權、有價值的資源或聲譽的損失）之外，網路釣魚也是最常見的網路攻擊。

網路釣魚活動的主要目標是**提高資安韌度**，並提供更適當的員工培訓，同時提供改進的回應和可衡量的結果。



所需時間

釣魚訓練可以持續一到十二個月。

透過定期培訓和練習可獲得最佳效果。



建議對象

受眾範圍可以很窄（對於捕鯨和魚叉式網路釣魚），也可以很廣。



執行方式

目的性的釣魚活動及適合的衡量措施

主要效益

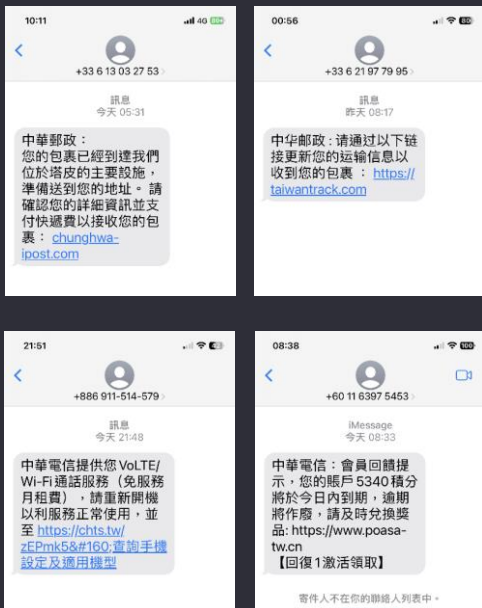
- 釣魚郵件是客製化的
- 真實性高
- 利用我們的威脅情報了解最新的網路釣魚情況
- 結合新的趨勢和技術，例如 QR code網路釣魚或欺騙攻擊(spoofing)

範例

- 事件場景：聖誕節禮物、團隊異地組織
- 流程相關場景：更新電子郵件訪問權限、車位預留
- 財務報告
- 反饋表

語音與簡訊攻擊 (Vishing and Smishing)

在針對電子郵件網路釣魚的強大保護措施的基礎上，攻擊者正在使用語音呼叫和手機文字簡訊來進行社交工程攻擊。



• Vishing and Smishing •

員工已經了解到電子郵件並不總是值得信任的，因此攻擊者逐漸將他們的惡意活動多樣化到語音電話和簡訊(vishing and smishing)。

我們模擬犯罪分子使用的相同攻擊手法，以確保對社交工程的持續防護。 Vishing可以透過自動錄音進行，也可以由真人進行。

主要效益

- 打擊網路釣魚“啟動”的元素
- 實現社交工程防禦的創新方法
- 應用高度個人化攻擊的可能性（通過事先的資料收集和攻擊計劃）

範例

- 快遞包裹
- MFA令牌
- IT Helpdesk
- Bonus / 禮物
- 技術支援
- 發票詐欺
- CEO詐欺



所需時間

一項活動通常會持續幾天到幾週，具體取決於目標受眾的規模和差異化需求。



建議對象

受眾可以是小眾，也可以是針對大眾。



執行方式

描述目標和所採用的攻擊技術、成功率以及觀察和建議的報告。

駭客攻擊實際演示 (Hacking Demos)

Hacking demos 是由道德駭客在觀眾面前現場進行的駭客攻擊，目的是演示網路攻擊的步驟，從而提高人們對危害人類行為的認識。



Hacking Demos

駭客演示以有形的方式展示了惡意行為者可以多麼容易地利用人和機器的某些漏洞。

它還可以激勵觀眾根據新觀察到的技術採取行動，並在某些情況下產生震撼因素(shock factor)。

駭客演示之後通常會進行資訊豐富的會議，從概念上撤回駭客攻擊的步驟，並介紹防止這些攻擊的最佳實務。

主要效益

- 真實透明的
- 互動性
- 直觀地說明攻擊的不同步驟

範例

- Online privacy
- 密碼政策
- 基礎設施安全
- 應用程式安全
- 資產管理



所需時間

一個駭客演示大概持續30 - 40 minutes.



建議對象

一般觀眾、目標觀眾或管理層

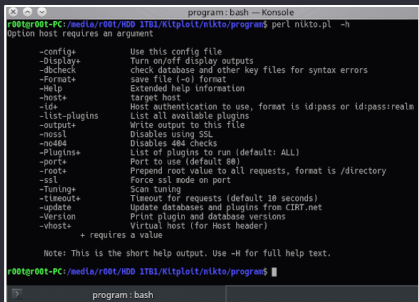
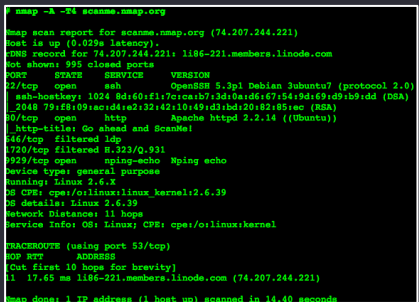


執行方式

駭客demo議程由 2位 執行者扮演駭客和受害者的專業人士。

駭客工具解析 (Hacking Tool Exhibition)

透過展示駭客的工具帶來教育和激發觀眾的想像力。



Hacking Tool Exhibition

除了筆記型電腦之外，駭客還依賴其他小工具來惡作劇。在演示過程，網路專家將揭開他們在過去的駭客攻擊中使用的工具，以惡意訪問建築物、網路、資產或資料。

透過互動式storytelling，參與者將能夠在一個全新的水平上與網路安全建立聯繫，並意識到安全遠不止是政策和培訓。

主要效益

- 多感官和觸覺學習
- 對網路隱藏面的獨特見解
- 灌輸好奇心
- 與大眾志願者進行現場演示的可能性

工具範例

- 鍵盤記錄器
- Proxmark II · RFID複製卡
- 感染惡意軟體的 USB
- 開鎖套裝
- Wi-Fi pineapple
- 惡意充電線



所需時間

駭客工具展覽是企業活動的完美補充，或作為安全意識月的展示一部分，可以設為一天。



建議對象

一般觀眾、特定族群

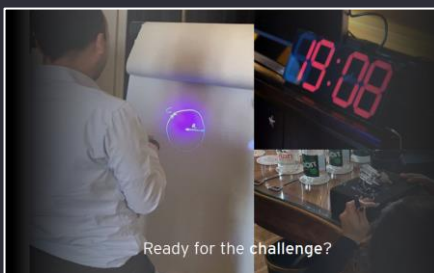


執行方式

間接動手網路安全演示，可以作為展台，也可以設置在會議室中。

密室逃脫 (Escape Room)

密室逃脫是一個，一群人被鎖在一個房間裡的互動式遊戲。為了逃脫，參與者在與時間賽跑中尋找線索並解決難題。



Escape Room

透過攻擊者的視角，或者透過徹底擊敗攻擊者，參與者了解網路安全的重要性，以及如何透過應用基本安全技巧來發揮作用。

而實境密室逃脫遊戲的興起，也提供企業一個**以群體建立為目標**的新鮮選擇，也是企業教育訓練靈活多變的素材，並且**提升員工參與度**，成為**組織培養互信**的黏著劑，也翻轉了外界對企業培訓的印象。

主要效益

- 遊戲化競爭
- Team building
- 訓練合作與溝通

範例

- 釣魚意識
- 資料移除
- 社交工程
- 實體安全
- 內部威脅
- 設備安全



所需時間

完成逃生室需要大約 40 分鐘，之後可以選擇進行 20 分鐘的匯報。



建議對象

一般受眾或管理層皆可。每支隊伍由4至6人組成。



執行方式

在辦公場所組織的密室逃脫活動或外部舉辦的活動，例如場外活動。

網路戰爭遊戲 (Cyber War Games)

網路戰爭遊戲代表了一種客製化的、身歷其境的、激烈的演習，以模擬關鍵的網路攻擊或事件。



Cyber War Games

網路戰爭遊戲模擬網路攻擊，旨在測試和訓練危機處理團隊正確應對未來的危機。

以實際、觀察到的現實情境為例，演習透過多媒體的加入來逼真地模擬網路事件的時間線和要點。

主要效益

- 量身定制的演習，對危機應對能力進行相關評估
- 允許驗證安全環境中的組織彈性。
- 促進即時(real-time)決策。
- 支持互動、反饋和公開討論。
- 培養事件管理和取證方面的經驗，提供最高程度的真實性和關鍵見解



所需時間

一個典型的練習約半天。



建議對象

聽眾通常是危機管理團隊、危機應對團隊或高層管理人員。

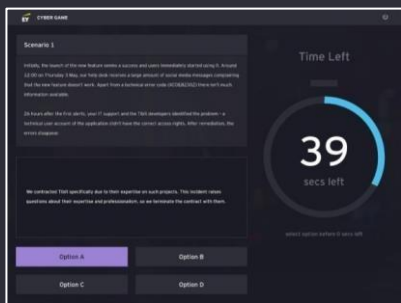
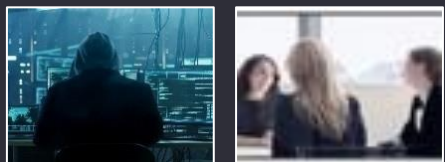


執行方式

一份關於良好做法、注意事項、改進的意見和建議的報告

商業遊戲 (Business Games)

在商業遊戲中，團隊在多輪比賽中競爭，以安全的方式實現商業目標。



Business Games

在限時的商業遊戲中，消除了與網路安全相關的大部分複雜性。

這不僅對遊戲中的任何人來說都很容易接觸資訊安全，而且還促使參與者思考對他們來說獲取資訊的重要性。

主要效益

- 鼓勵觀眾參與
- 使網路安全成為一個平易近人的話題
- 促進資訊共享
- 發展資安知識

範例

- 幾種商業遊戲場景可滿足您組織的特定要求。
- 例如：玩家是一家純網路銀行公司的負責人，同時必須應對資訊安全挑戰和財務問題。



所需時間

商業遊戲和說明，包括後續經驗討論，總共持續約 2 小時。



建議對象

這些商業遊戲主要針對管理層和董事會。



執行方式

線上或在您的辦公場所組織的商業遊戲活動。

3

結論與建議

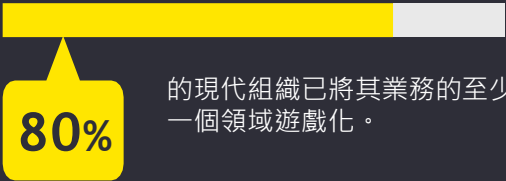
成功的資安意識計劃主要有三大支柱面向

成功的意識計劃能以持續的方式激勵和吸引人們。

意識宣傳工作應將交給專業

採用創新的意識方法來積極培訓和吸引用戶，而不是教條式的方法。

將學習科學、神經認知科學、網路使用者同理心(cyber user empathy)、行為科學和遊戲化中通常被忽視的技術和方法結合起來，以優化用戶體驗。



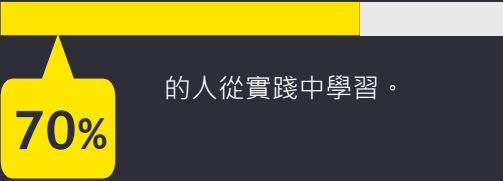
Source: Gartner, “Gamification 2020: What Is the Future of Gamification?”.

認知意識是一種持續的努力

“一次性”意識練習不太可能將安全行為嵌入人們的日常生活中。

為了取得成功，意識計劃需要積極致力於行為改變。

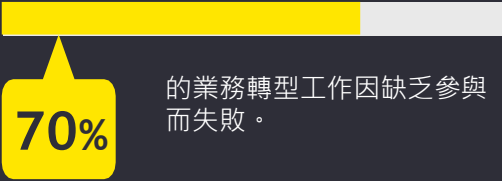
針對意識努力的重複出現與邊做邊學會和團隊動力交織在一起，增加了這種改變的機會。



Source: 70/20/10 Institute, “What is the 70/20/10 model?”.

每個意識計劃都是獨特的

資安意識計劃需要由實際業務風險驅動，以符合組織的需求並提供最佳定制解決方案，同時與現有的組織環境和文化保持一致以優化採用行為。



Source: Gartner, “2017 Trends in Global Employee Engagement Study”.

成功的資安意識計畫四要素及安全文化

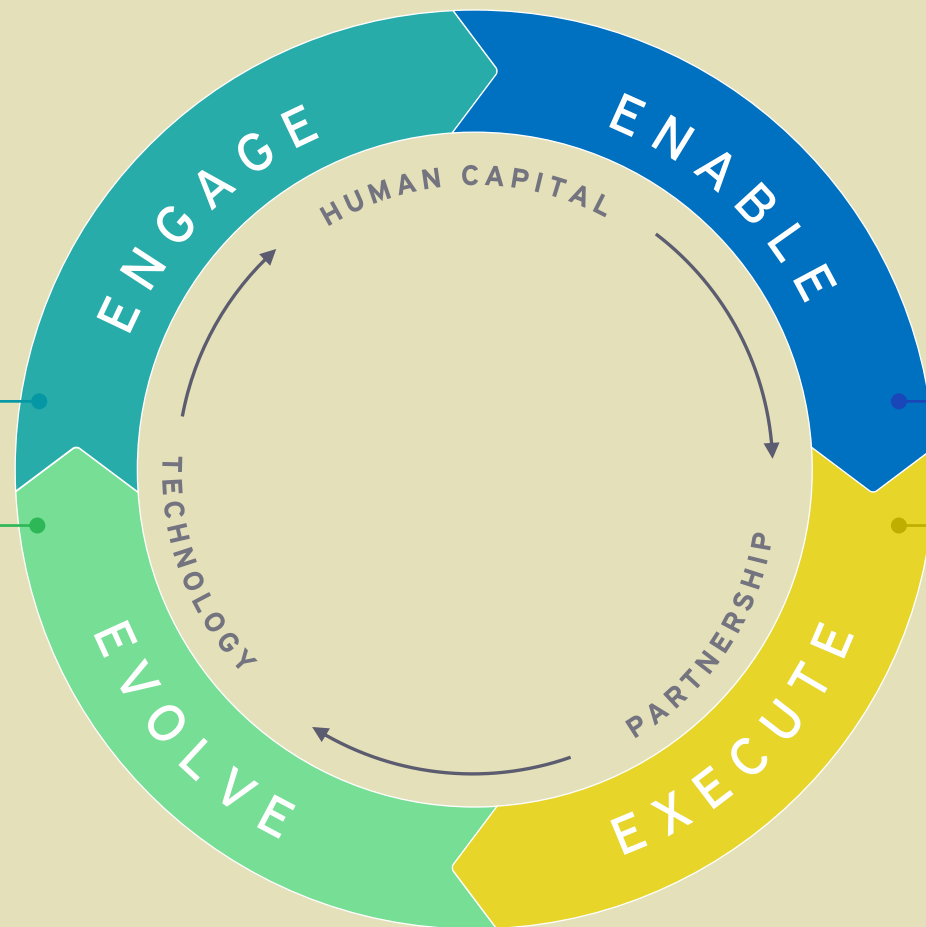
- ▶ 降低基於人產生的網路風險，並在獨特的商業環境中加強安全文化

ENGAGE

創建基於角色和風險的活動與溝通，
以在正確的時間向正確的人傳遞正
確的信息，以實現所需的安全行為

EVOLVE

安全文化建立在與安全團隊成
員的信任、有效溝通和正面經
驗之上



ENABLE

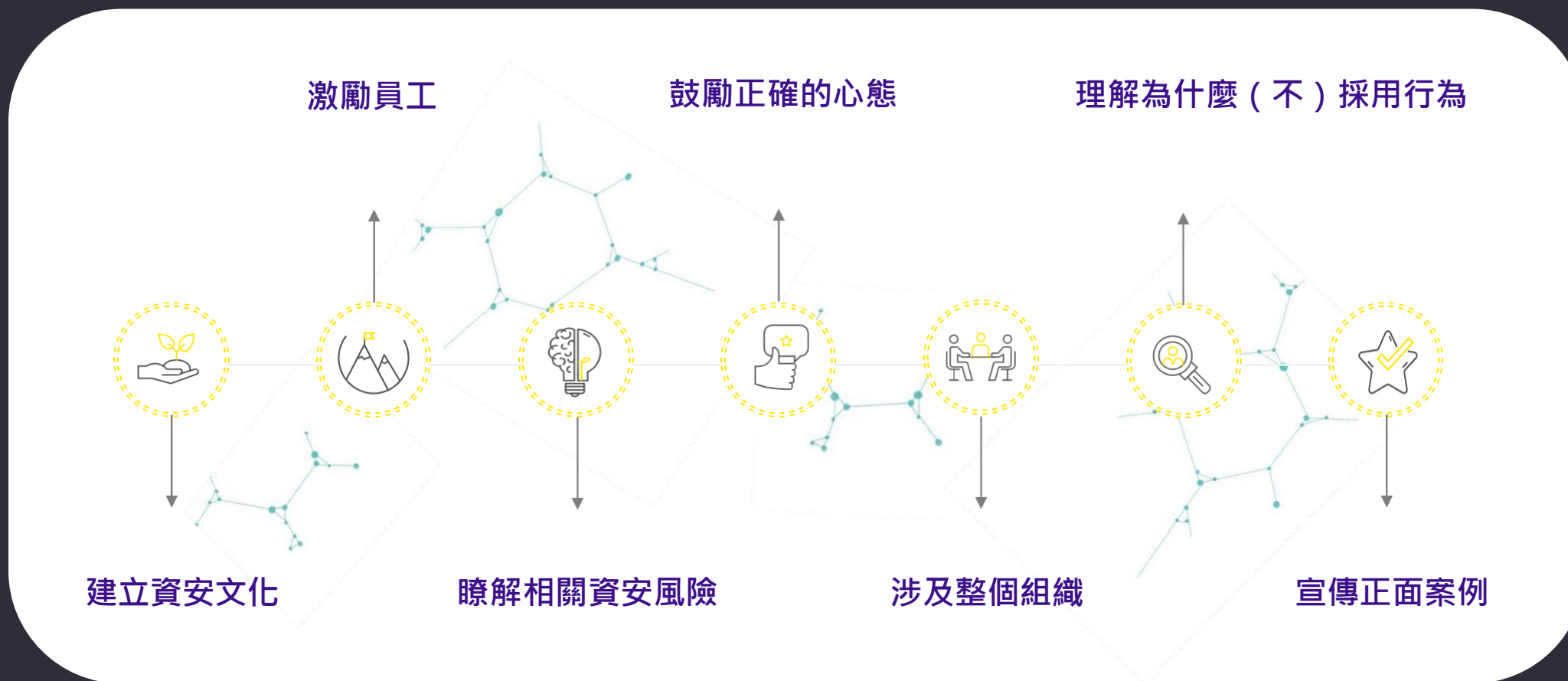
為員工提供知識和工具，以示範適當
的安全行為並在面臨挑戰時做出適當
的選擇

EXECUTE

將網路安全整合到企業的角色和日常
生命週期中，使員工能夠展示適當的
安全行為和網路安全策略

建立以安全為導向的組織文化、鼓勵正確的心態

- 讓整個組織參與資安意識過程來實現長期的行為上的改變。



“

資安尚未成功，

同志仍須努力！

安永 | 建設更美好的商業世界

安永的宗旨是致力建設更美好的商業世界。我們以創造客戶、利害關係人及社會各界的永續性成長為目標，並協助全球各地資本市場和經濟體建立信任和信心。

以數據及科技為核心技術，安永全球的優質團隊涵蓋**150**多個國家的業務，透過審計服務建立客戶的信任，支持企業成長、轉型並達到營運目標。

透過專業領域的服務 - 審計、諮詢、法律、稅務和策略與交易諮詢，安永的專業團隊提出更具啟發性的問題，為當前最迫切的挑戰，提出質疑，並推出嶄新的解決方案。

加入安永LINE@好友
掃描二維碼，獲取最新資訊。



安永是指 Ernst & Young Global Limited 的全球組織，加盟該全球組織的各成員機構都是獨立的法律實體，各成員機構可單獨簡稱為「安永」。Ernst & Young Global Limited 是註冊於英國的一家保證（責任）有限公司，不對外提供任何服務，不擁有其成員機構的任何股權或控制權，亦不作為任何成員機構的總部。請登錄ey.com/privacy，了解安永如何收集及使用個人資料，以及個人資料法律保護下個人所擁有權利的描述。安永成員機構不從事當地法律禁止的法律業務。如欲進一步了解安永，請瀏覽 ey.com。

安永台灣是指按中華民國法律登記成立的機構，包括：安永聯合會計師事務所、安永管理顧問股份有限公司、安永諮詢服務股份有限公司、安永企業管理諮詢服務股份有限公司、安永財務管理諮詢服務股份有限公司、安永圓方國際法律事務所及財團法人台北市安永文教基金會。如要進一步了解，請參考安永台灣網站 ey.com/zh_tw。

© 2022 安永諮詢服務股份有限公司。
版權所有。

APAC no. (請填上SCORE number)
ED MMY [填寫圖片版權到期日，若無到期日請寫上 ED None; 若無圖片請刪除]

本材料是為提供一般信息的用途編製，並非旨在成為可依賴的會計、稅務、法律或其他專業意見。請向您的顧問獲取具體意見。

ey.com/zh_tw