CYBERSEC 2021
臺灣資安大會

ORGANIZED BY iThome

TRUST:redefined

信 任 重 構

MAY 4-6 臺北南港展覽二館

CYBERSEC 2021
臺灣資安大會
ORGANIZED BY iThome

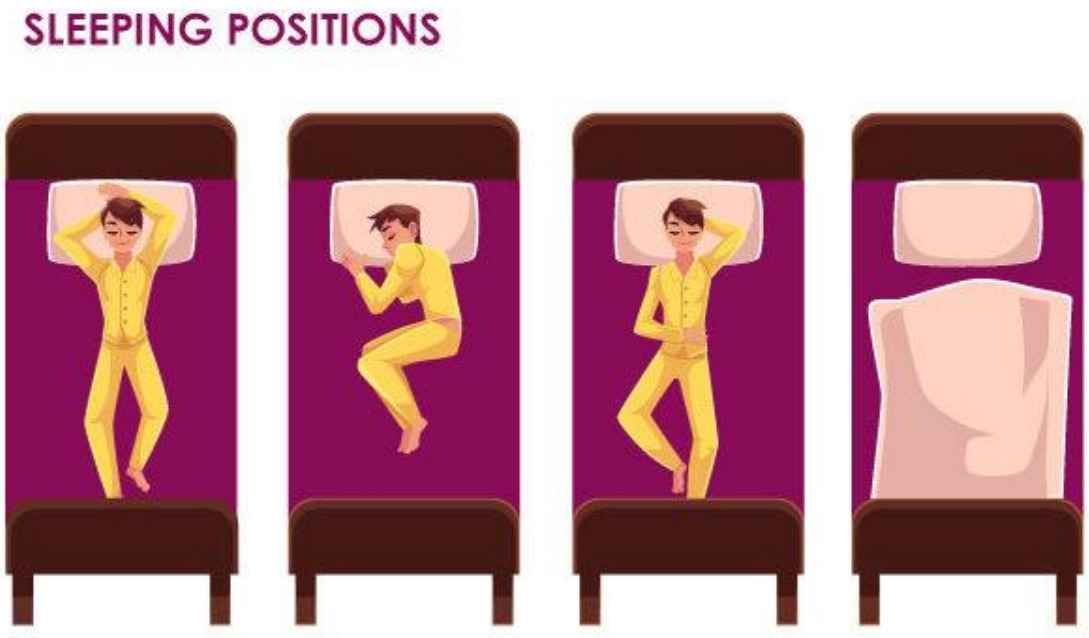
TRUST:
redefined

金融資安論壇

資安落實的有效性經驗分享

玉山銀行資安長 陳榮俊

MAY 4-6 臺北南港展覽二館



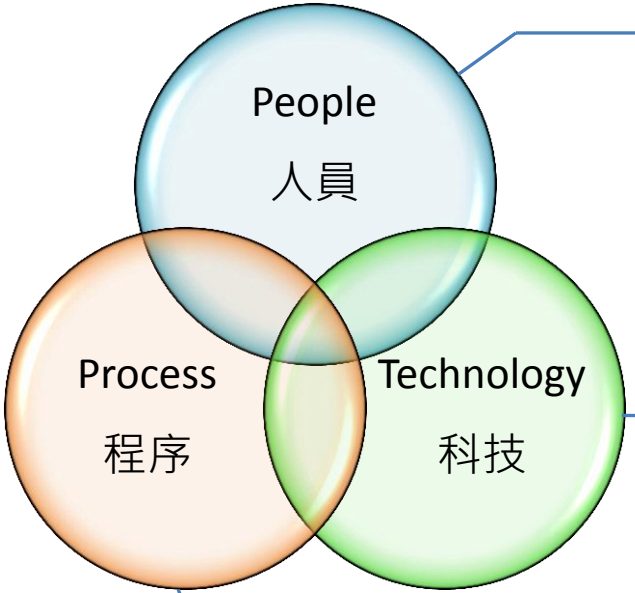
圖片來源：https://www.cyberseer.net/8-reasons-for-mssps-to-detect-security-incidents/

TRUST: redefined

資安落實面臨的挑戰

相信大家都有這樣的感慨，該訂的規範都訂了，該買的資安設備都買了，該做的教育訓練也都做了，為什麼老闆問起我們的資安做得好不好，大家還是沒有信心？

建構完善資訊安全系統的三要素



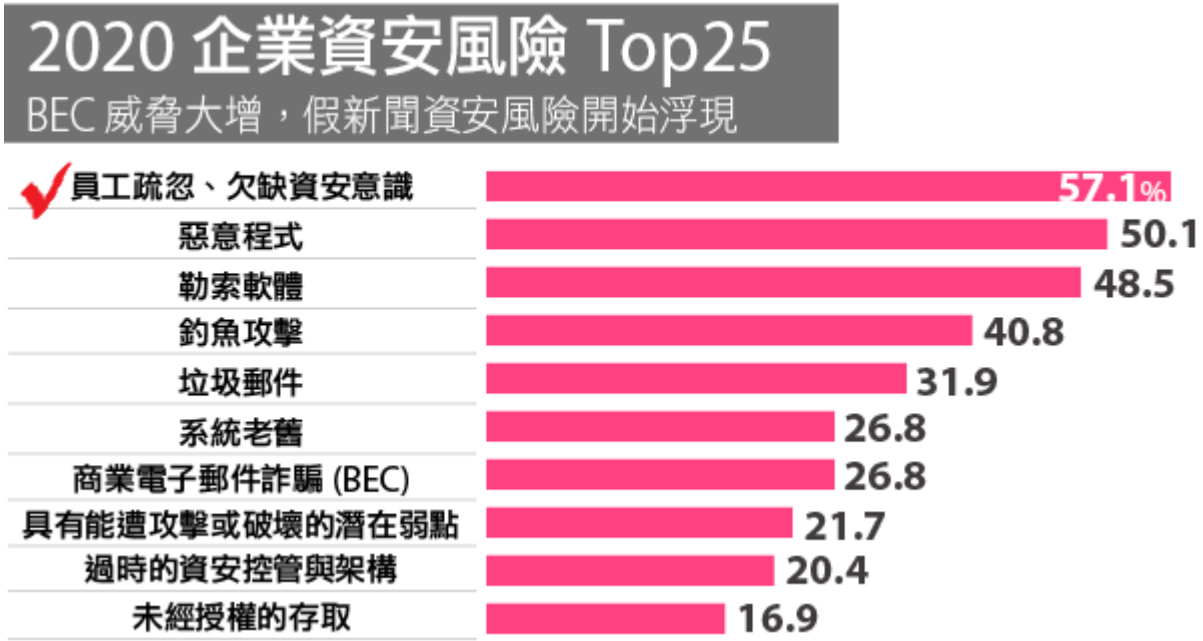
培育人才

發展資訊

建立制度

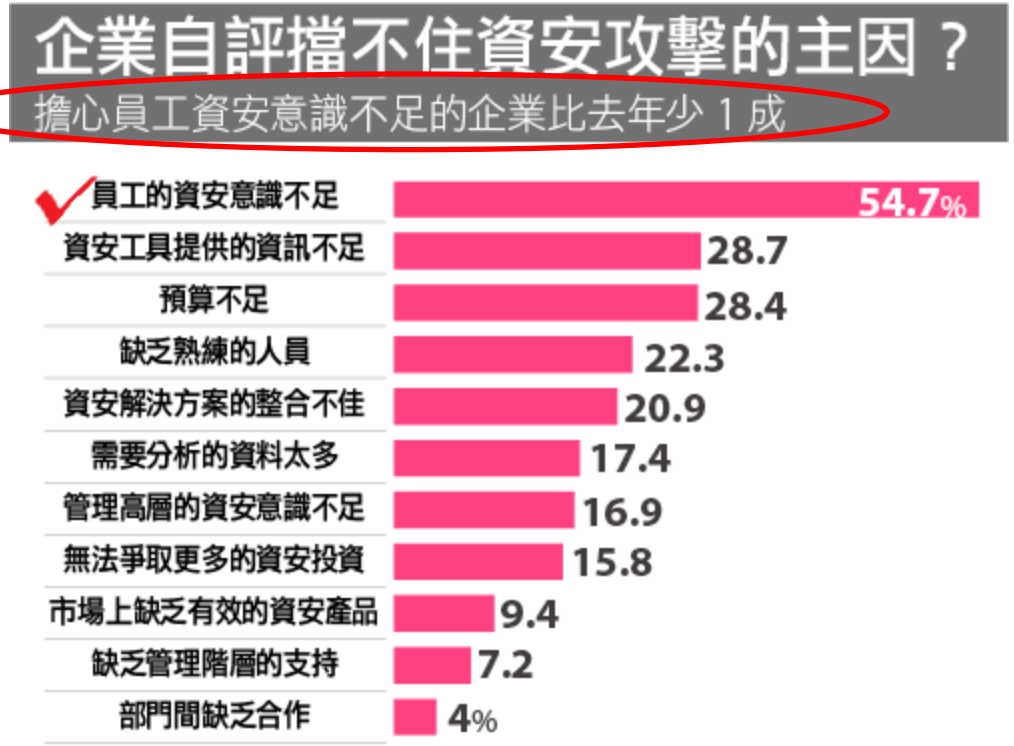
有做≠做得好、做到位

資安落實面臨的挑戰-人員 1/5



圖片來源：https://www.ithome.com.tw/article/139493

資安落實面臨的挑戰-人員 2/5



圖片來源：https://www.ithome.com.tw/article/139495

資安落實面臨的挑戰-人員 3/5

小和尚唸經，有口無心.....

- 豐富多樣的課程，如影片、漫畫、workshop
- 有考試就會有壓力
- 用團隊的力量來要求(分組共責)

資安落實面臨的挑戰-人員 4/5

不是不知道，就是不小心.....

- 以風險導向機制決定訓練的頻次
- 列入平日考核紀錄，與績效連結
- 透過制度的輔助，如流程控管、checklist

資安落實面臨的挑戰-人員 5/5

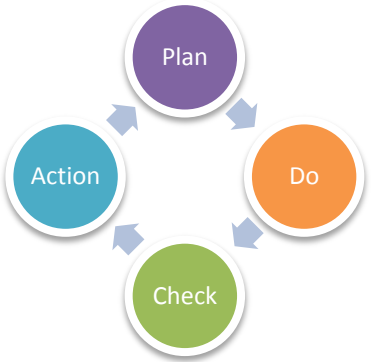
不是做不到，而是人力不足，能力亦有待加強.....

- 找不到現職人員，就從新人開始培養
- 透過團隊學習提升能力，如讀書會、分組技術研討
- 與一、二道防線進行輪調實習，深耕一、二道專業能力

資安落實面臨的挑戰-程序 1/2

無法面面俱到，至少掌握全貌.....

- 對標國際標準，建立ISMS運作機制(ISO 27001)
- 透過不同框架，檢視不同面向：NIST CSF、MITRE ATT&CK
- 透過資安成熟度評量，建立PDCA良性改善循環機制



資安落實面臨的挑戰-程序 2/2

雖然有SOP，但就是有人會便宜行事.....

- 凡走過必留下軌跡，達到嚇阻作用
- 透過查核制度(自行查核、內外部稽核)找出害群之馬
- 流程中的重要關卡設控制點

資安落實面臨的挑戰-科技 1/2

產品琳琅滿目，哪一個才是Mr. Right？

- 多看、多聽、多交流：廠商研討會、媒體(iThome)、同業互動
- 發掘痛點，自行設計POC情境
- 確定要掌握的關鍵核心能力，決定資源投入的方式
- 資源有限，導入新產品也要檢視現有防禦機制是否有功能重複

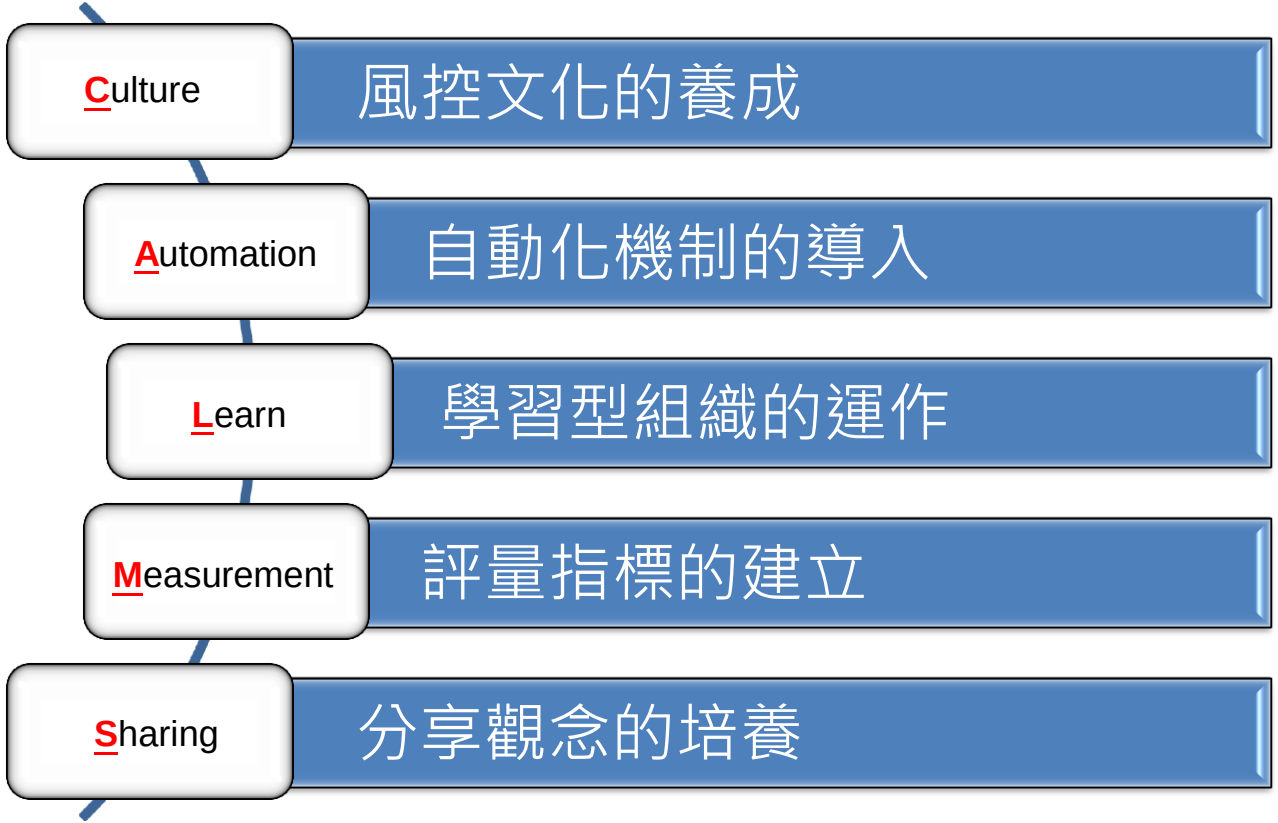
資安落實面臨的挑戰-科技 2/2

如何確保Mr. Right永遠都是Right？

- 定期檢視 + 監控機制
- 以駭客角度檢視防禦破口：紅隊演練
- 無法100%保證沒有問題，但可以透過風險轉嫁：投保資安險

CALMS Model

成功關鍵



TRUST:
redefined

感謝聆聽　敬請指教