



數位轉型下的資安挑戰 :企業需求與人才機會

CYBERSEC 2025





- 專注於滲透測試、弱點掃描、資安健診及社交工程演練等資安檢測服務領域，從業期間已負責 **80+** 家企業客戶
- 滲透測試服務經歷涵蓋 **航空業、金融業、政府機關、電子商務、電子支付、科技業、製造業、遊戲業** 等廣泛領域
- 精通**網路應用服務、網頁 API、行動應用 APP**之滲透測試

Experience

- 雲力橘子 - 資安服務部 經理
- 果核數位 - 資訊安全部 副理
- 詮睿科技 - 資訊安全處 資安顧問
- 果核數位 - 資訊安全部 資安工程師

Certificate

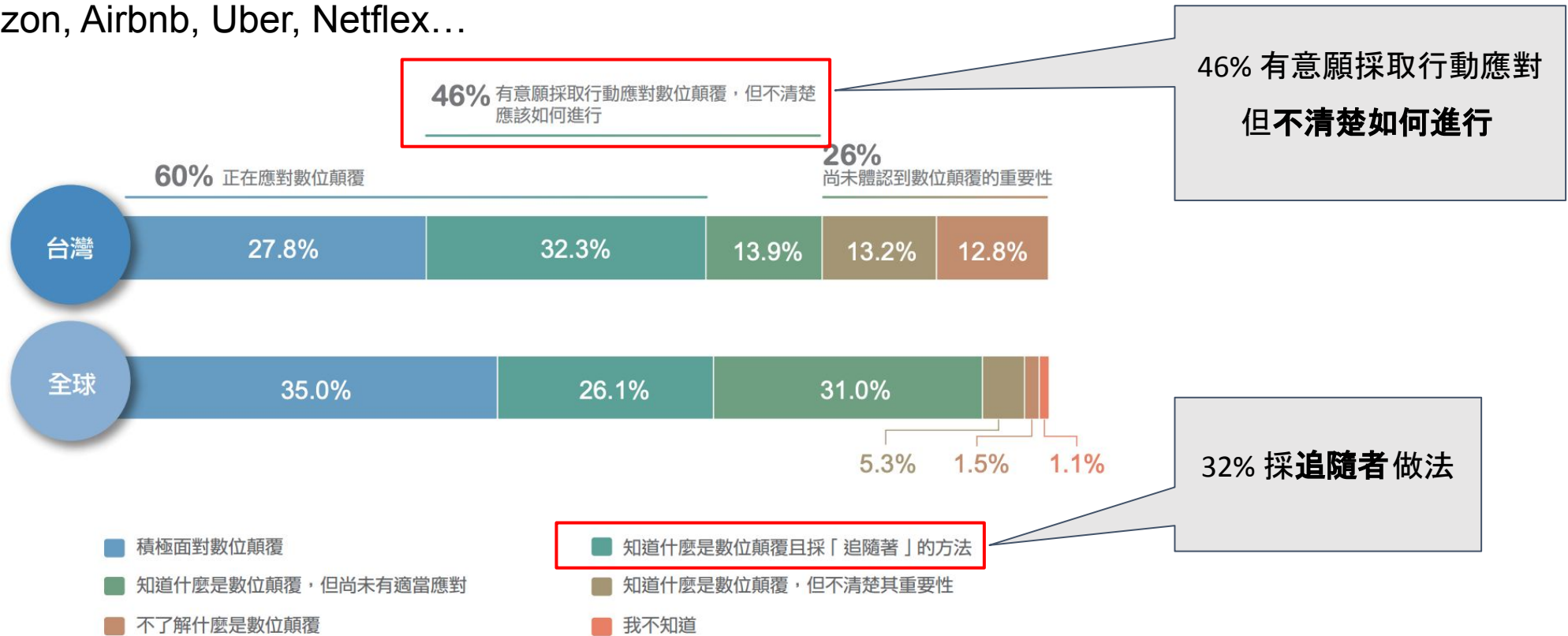
- LPT - Licensed Penetration Tester
- CPENT - Certified Penetration Testing Professional
- ECSA - EC-Council Certified Security Analyst
- CHFI - Computer Hacking Forensic Investigator
- CEH - Certified Ethical Hacker
- ISO 27001:2022 LA - Information Security Management Systems Auditor/ Lead Auditor

- 數位轉型的趨勢與背景
- 數位轉型下的資安挑戰
- 企業的資安人才需求與發展機會

數位轉型的趨勢與背景

數位顛覆能在一夕之間顛覆市場上的既存企業並重新塑造市場，透過新的數位科技與商業模式對公司現有價值主張及其最終市場定位造成衝擊。

Ex: Amazon, Airbnb, Uber, Netflix...



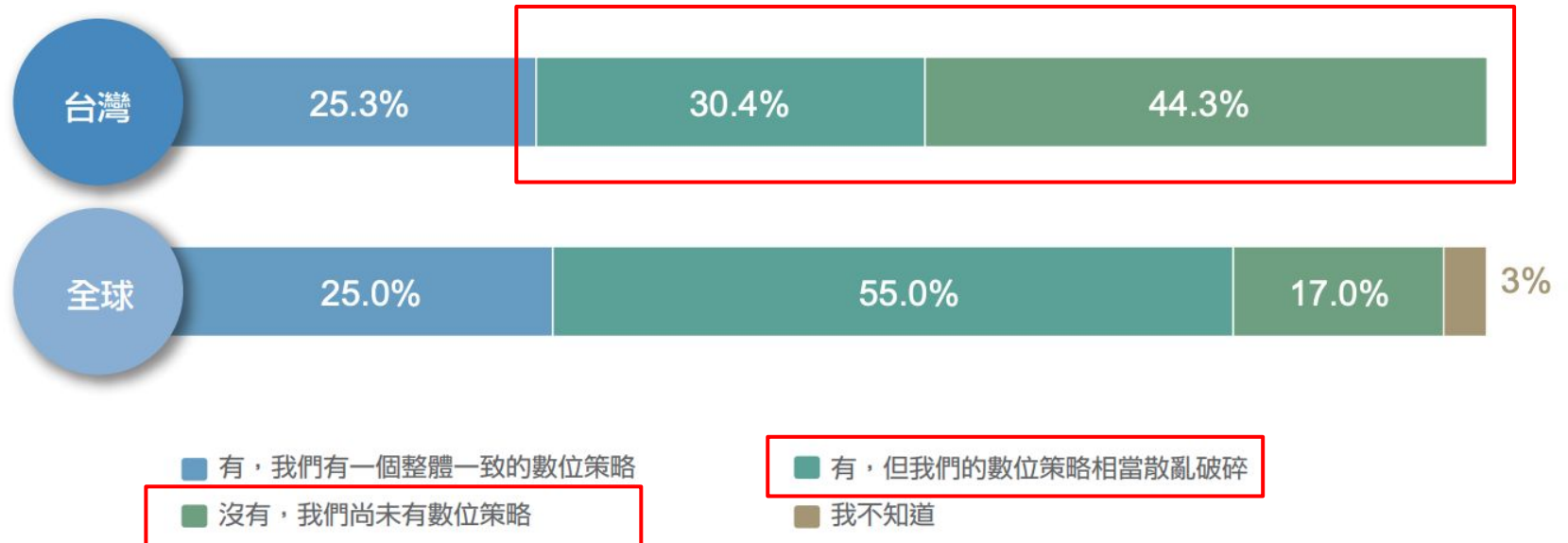
數位轉型的趨勢與背景

數位化策略 → 被市場拖著走

- 上市上櫃公司
- 供應鏈攻擊：上下游廠商
- ISMS 導入

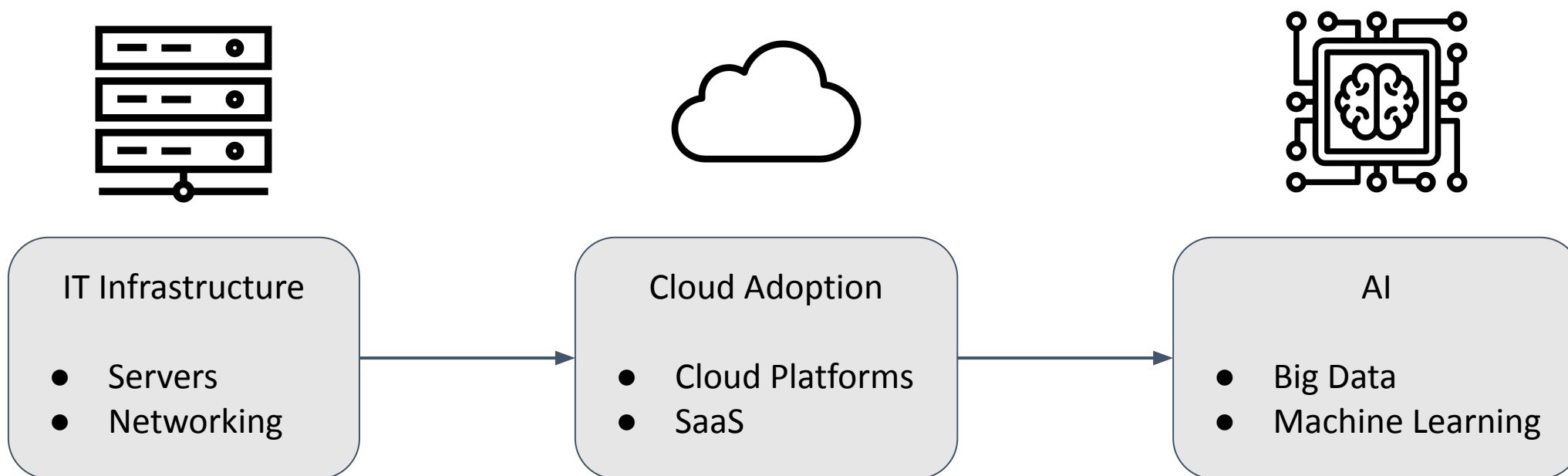
台灣 75% 企業

- 有策略，但很破碎
- 沒策略



資料來源：資策會MIC、全球商業數位轉型中心（Global Center for Digital Business Transformation），2023年5月

企業數位轉型是必然，雲端、數據、AI、遠端工作全面普及，商業快速變革，連帶**風險巨增**



數位轉型下的資安挑戰

- 雲端化、遠端辦公、資料外洩、勒索病毒...
- 過去 → 防火牆、弱掃、防毒
 - 有弱點, 但不修也沒關係
 - 防火牆規則很寬鬆
 - 防毒偵測結果不會持續追蹤
- 現在 → 滲透測試、資安治理、EDR、持續監控...
 - 面對弱點, 但不知道怎麼修? 不能修又怎麼辦?
 - 沒有監控人員?
 - 沒有治理人員?
 - 想上雲, 但不懂雲架構?
 - 開發人員, 但不懂開發安全?

2024 臺灣企業轉型現況及需求調查(資誠 PwC Taiwan)

- 調查對象:涵蓋服務業、製造業、農業、陸上運輸業、醫療保健及社工服務業
- 數位轉型目的:60% 的企業以提升作業效率為主要目標
- AI 應用現況:90% 的企業尚在尋找 AI 的切入點,處於萌芽階段
- 資安意識:60% 的企業已使用高等數位工具

臺灣企業轉型面臨的挑戰

45.5%

害怕投入的資金
無預期成效

24.5%

市場上工具或
解決方案價格
難以負擔

23.2%

數位技術自主
不足,維運仰賴
資服業者

資安不是只需要攻擊手

- 滲透測試、紅隊演練
- 漏洞修補、弱點管理
- 資安監控、事件應變措施
- 雲端與架構安全設計
- GRC(治理、風險、法規)

- 沒有 100% 的安全, 也沒有 100% 的防禦率
- 駭客不是資安專家

領域	關鍵技能	對應職位
紅隊/攻擊方	紅隊演練、滲透測試	資安滲透測試工程師、紅隊工程師
藍隊/防禦方	Log 分析、事件調查	資安事件應變工程師、資安監控分析師
雲端安全	雲端安全架構	雲端資安工程師、資安架構師
開發安全	AppSec、Secure Coding	應用系統安全工程師、DevSecOps 工程師
政策/治理	資安框架、法規遵循	資安治理顧問、資安風險管理師



Thank you.