VIVOTEK
A Delta Group Company

2023 資訊系統安全風險管理執行報告

Presenter: Perkins, Director

July 27, 2023

全年概況

- 資訊技術和資訊基礎架構進行優化改善
  - 由台達協助完成基礎架構資安評估

- 建立資訊安全政策和基礎規範
  - 取得 ISO 27001 認證 – 2022/8 取得證書
  - 完成 ISO 27001 年度複查 – 2023/6/8

- 保障重要資訊資產和設備安全
  - 強化端點管理，移除非必要端點系統管理權限
  - 重要伺服器的資安定位 MDR 建置 – 有找出疑似攻擊事件，並已經進行處理

- 本報告已經於 2023/7/27 日於董事會報告

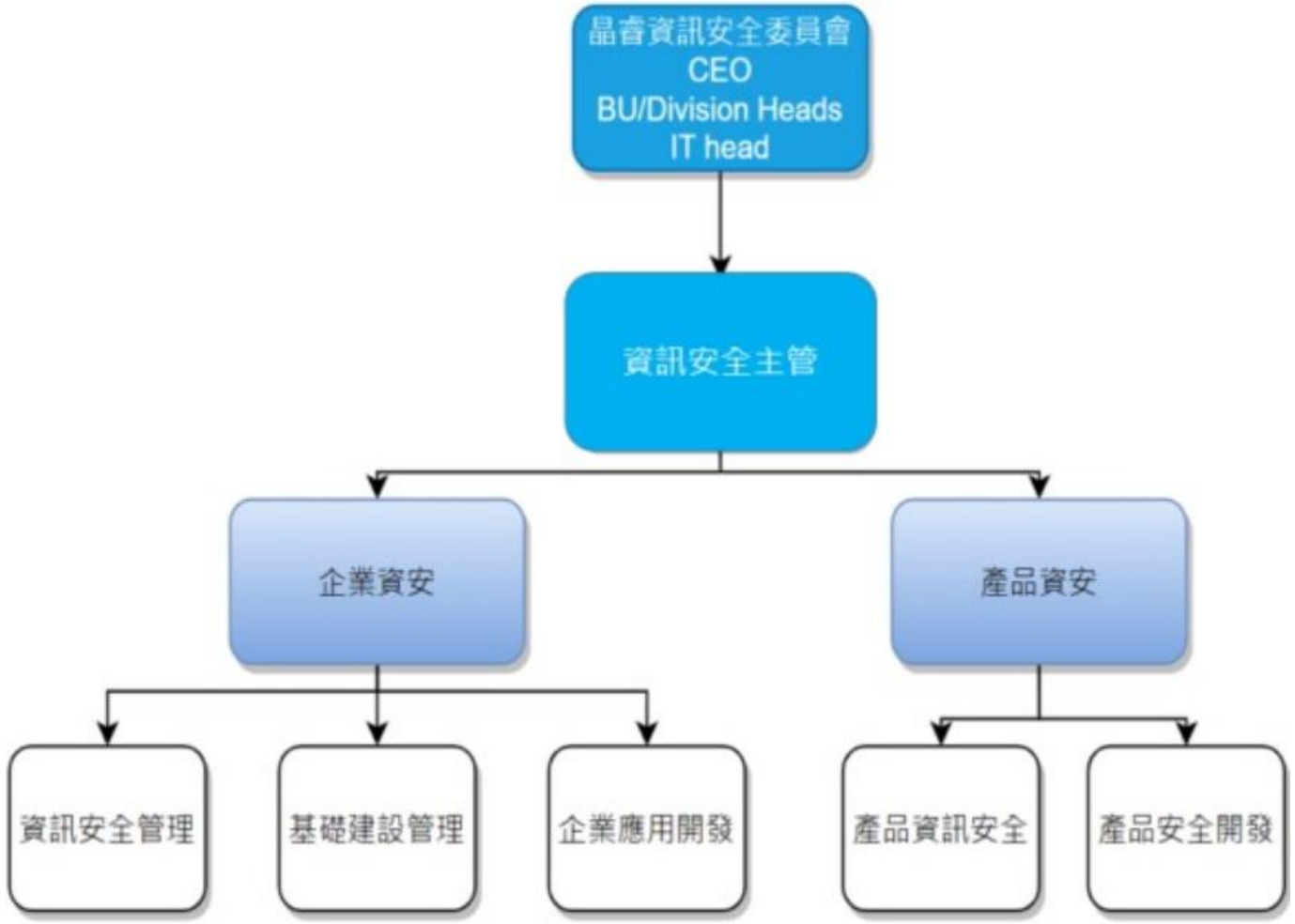
2023 挑戰

- 外部攻擊
  - 網站漏洞
    - 有兩件中度安全漏洞，因為不易被利用，目前持續觀察中
  - 社交工程和針對高階主管的APT持續攻擊
    - 持續有發現針對高階主管帳號的針對性攻擊和釣魚信件

- 內部挑戰
  - 基礎設施和電力供應的穩定性
    - 不能完全排除電力供應問題，以及其他自然災害對營運資訊服務的影響，必須有效配置資源，尤其針對伺服器端進行保護，保障意外發生時重要資訊服務不中斷
  - 台達網路整合
    - 技術防護上面逐步強化，朝零信任架構處理
    - 整合可用資源，拉高資訊投資的ROI
  - 全球性內部服務可用性
    - 強化雲端系統使用，緩解VPN 的限制和依賴

資訊系統安全策略

- 強化資訊安全組織
  - 晶睿資訊安全委員會於 2020 年 1 月正式成立，主委由總經理擔任，委員則由各單位一級主管擔綱。主要任務為資訊安全政策制定、資訊安全維護、資訊安全架構制定、系統弱點掃描、產品資訊安全審核等。資訊安全委員會於2021年設有資安主管及專責資安人員定期於每年 12 月舉行會議，檢討資訊策略，與當年資安執行成果，並制定下個年度的資安工作要點，再交由資訊安全團隊實現目標。
  - 2023年會持續依照這個架構運行資訊安全和資訊服務



資訊系統安全政策

- 資訊安全政策
  - 「確保業務資訊安全、保障業務持續營運」
  - 適用於所有同仁、臨時契約人員、委外廠商，使用本公司資訊資產之外部組織人員
- 要求
  - 不侵犯智慧財產權，提出大型AI服務的使用範圍政策規範
  - 不安裝和使用任何沒有適當授權的軟體或服務於業務上
  - 安裝防毒軟體和DLP防護
  - 資訊設備遺失需透過規劃的流程盡速回報降低資訊資產遺失的損害
  - 公司電子信想僅作公司業務使用
  - 未經授權允許，不得接露公司業務資訊與秘密
  - 善加保管公司資訊系統帳號密碼
  - 迅速回報任何資安事件與網安事件

2023 年度上半資安執行報告

- ISO27001 ISMS系統和標準認證執行結果
  - BSI於2023年6月來訪進行外部持續稽核
    - 基於ISO 27001:2013標準，發現次要缺失4項
    - 沒有主要缺失
    - 主要集中於
      - 防火牆設定備份還原演練未執行
      - 端點技術脆弱點管理機制未臻完全
      - 營運持續演練活動未執行
      - 部分系統帳號權限清查未執行

- BSI 於2023持續稽核結果，認定ISO 27001證書持續有效

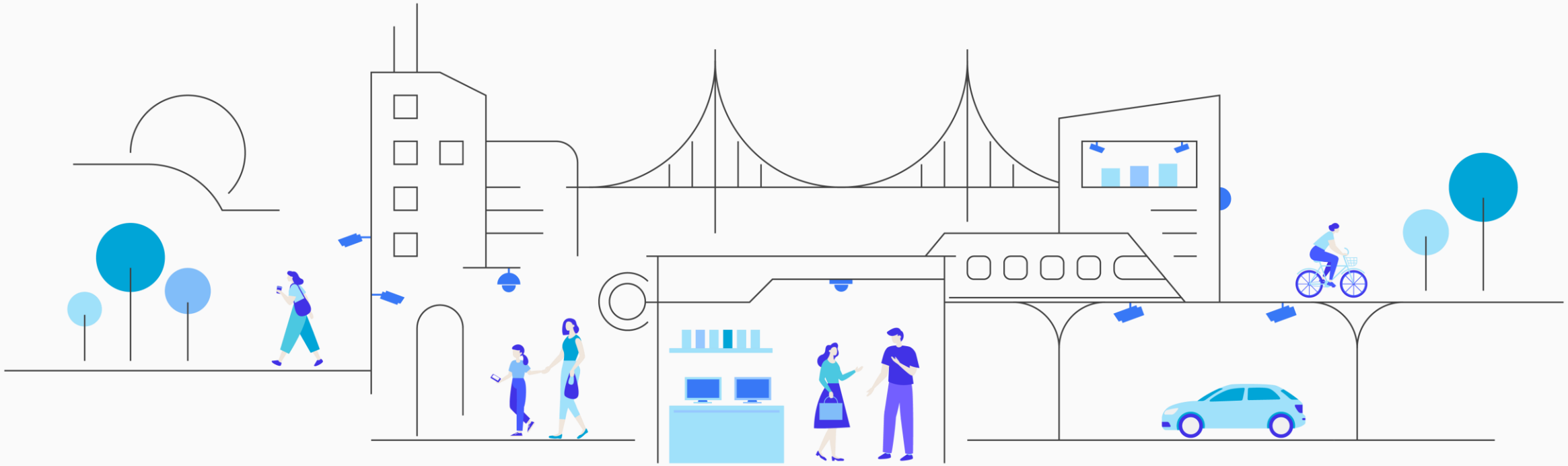
2023 年度資安執行報告

- 投入資源
  - 資安人員一位持續資訊安全管理系統維運
  - 投入4個人力持續對網路系統和基礎建設強化技術安全和可用性維運
  - 投入4個人力針對網路應用服務，包含ERP和網站系統進行安全開發，保障商業應用安全
  - 教育訓練
    - 全組織資訊安全教育訓練
      - 95.4% 參與現場或線上(錄影)訓練
      - 平均 每人訓練時數 1.03 hours

2023 年度資安執行報告

- 執行事項
  - MDR 建置 – 廠商於 POC 期間通報有疑似駭客活動
    - 已針對該事件進行調查
    - 對遭植入特殊帳號的伺服器進行更新補洞
    - 特殊權限帳號清除
  - Local Admin 權限回收
  - VPN 只針對需要且有申請用戶開放
  - 作業系統持續更新，修補可能漏洞
  - Confluence 伺服器版本更新，避免漏洞被利用
  - 產線網路切換到台達產線網段，與辦公室網段切離

Thank You for Your Attention.



VIVOTEK
A Delta Group Company

We Get The Picture