VIVOTEK
A Delta Group Company

2024 資訊系統安全風險管理執行報告

Presenter: Perkins, Director

July 29, 2024

全年概況

1

2023 Q3

- 針對台達 IT 資安評估，進行系統改善，主要是 168 機房環境

2

2023 Q4

- 開始 DLP log 定期 review，確保無異常資料轉移

3

2024 Q1

- 192 機房冷氣改善、汰舊換新，降低系統無法使用風險

4

2024 Q2

- 完成 ISO 27001 年度複查，並準備明年度改版 ISO27001 2022
- 完成國泰資安險評估對外網站安全漏洞修復

2024 資安挑戰

1 網站漏洞

共有兩件，網站更新有急迫性

2 帳密外洩事件

與台達網路高度相依，且 AD 帳號高度整合各應用，帳密外洩，造成的影響也變得深遠，啟動 MFA 刻不容緩

3 法規遵循的複雜性

全球各地不斷更新的資訊安全要求和資料保護法規，如GDPR和IEC62443, ISO27071, ISO 27017/27018，給我們的合規工作帶來了巨大壓力。我們需要持續關注法規變化並及時調整我們的政策。

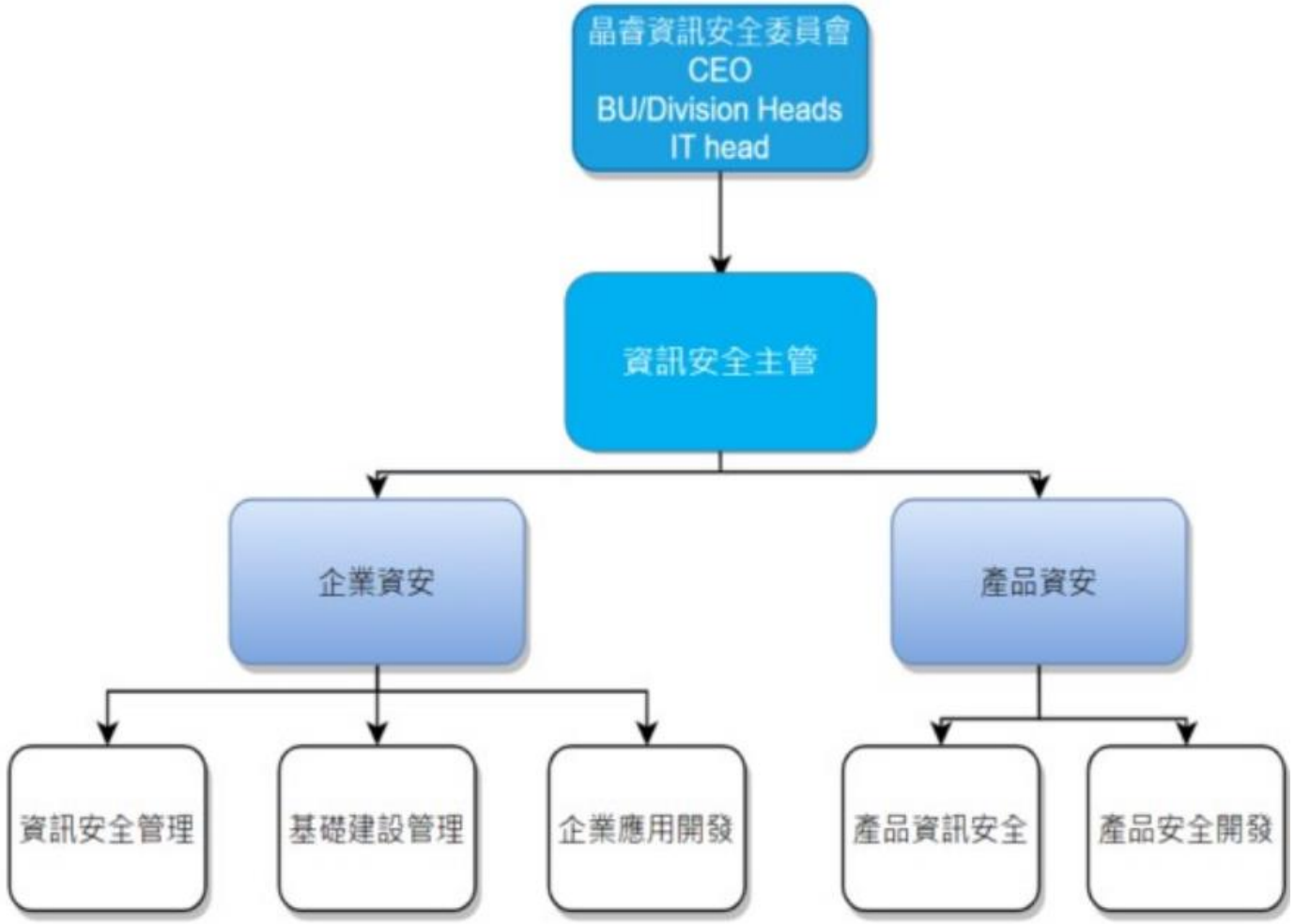
4 供應鏈與子公司安全風險

隨著供應鏈與子公司與我司系統整合性變高，安全性管理變得越來越複雜。Security Baseline 的與時俱進和執行上的確實要求相當關鍵。

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。

  - 2024年會持續依照這個架構運行資訊安全和資訊服務
  - 此報告已經於 2024/7/29 向董事會報告



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

2024 年度資安執行狀況

- ISO 27001 年度複查
- 作業系統持續更新，修補可能漏洞
- 168 機房環境改善
- 國泰資安險對外網站漏洞修補

ISO27001 認證年度複查

1

BSI外部稽核

2024年5月，英國標準協會（BSI）來訪進行外部持續稽核，基於ISO 27001:2013標準進行全面評估。

2

稽核結果

稽核結果相當不錯，我們沒有被發現主要或次要缺失。審核員提出了三點建議，主要與文件管理相關。

3

證書持續有效

基於稽核結果，BSI認定我們的ISO 27001證書持續有效，肯定了我們在資訊安全管理方面的持續努力。證書效期將到 2025/12 月。

4

未來改進

我們已著手調整文件管理流程，以適應即將實施的ISO 27001:2022版本要求，確保我們持續符合最新標準。

持續性安全維護

1 作業系統更新

我們持續進行作業系統的更新和補丁管理，及時修補已知漏洞。這個過程涵蓋了所有公司設備，包括服務器、個人電腦，確保我們的系統始終處於最安全的狀態。

2 168機房環境改善

我們對168機房進行了環境改善。這包括優化電力供應、加強物理安全措施等。這些改進增強了我們的整體資訊安全防護能力。

3 國泰資安險網站漏洞修補

針對報告內的對外網站進行修補或關閉不必要的對外網站，讓外部可利用弱點進一步降低。

2024年度資安執行報告：投入資源

Infra 人員

4 位

App/ERP 開發維護人員

6 位

資安人員

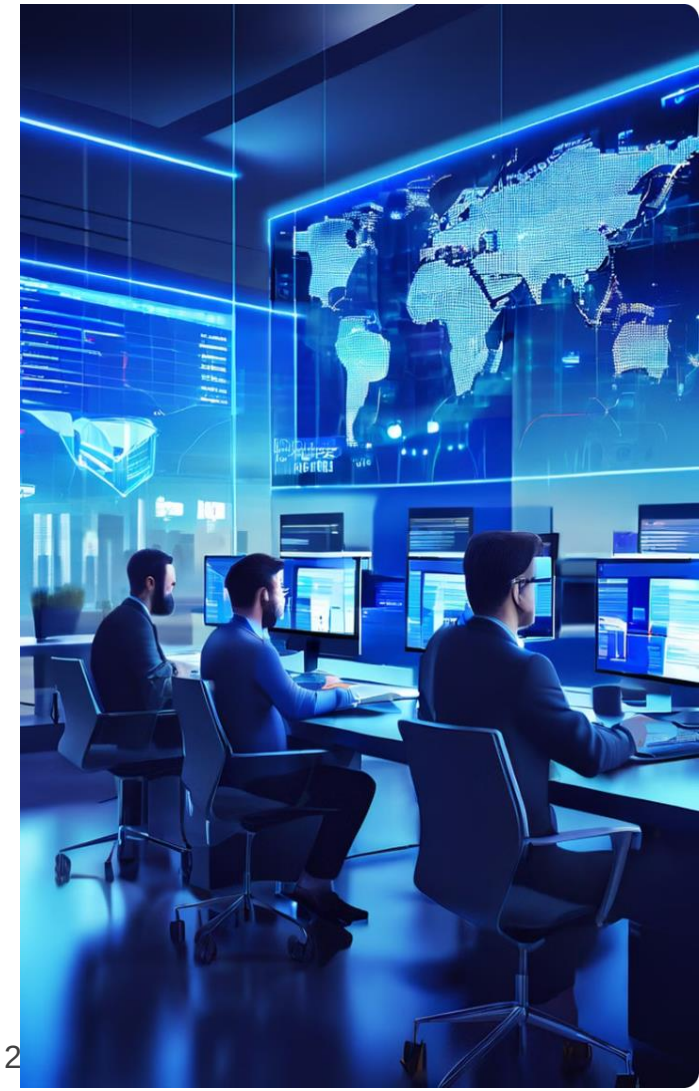
1 位

全組織人均教育訓練時數

1.25 hours

全組織教育訓練比例

90%



2024年度資安執行報告：成果與進展

指標	2022	2023	改善幅度
同仁參訓廣度	97%	90%	-7.2%
同仁參訓深度	1 h	1.25 h	+25%
風險處理的及時性(評估為風險項目的是否按時完成)	33%	100%	+203%
保留監控之高風險數量	0	2	-
矯正處理的及時性(稽核項目是否按時完成矯正)	100%	61%	-39%
資安事故	0	2	-
應用系統可用性	99%	99.7%	+0.7%
基礎建設可用性	99%	99%	+0
環境可用性	99%	99%	+0

展望未來：2024 下半年到 2025上半年資安規劃

3	4	1	2
系統安全升級	ISMS 有效性內部稽核	稽核問題持續改善	ISO 27001:2022 驗證
NDR ExtraHop導入	組織資訊安全風險評鑑	全組織技術脆弱點管理	取得新版憑證
CyberArk特權帳號管理	營運持續計畫演練	稽核問題改善與複查	
Mac安全措施	資訊資產年度盤點		

網路系統安全升級

NDR ExtraHop導入

我們即將導入了網絡檢測和響應（NDR）系統ExtraHop。這個先進的系統能夠實時監控網絡流量，快速識別和響應潛在的安全威脅，能夠大大提高了我們的網絡安全防禦能力。

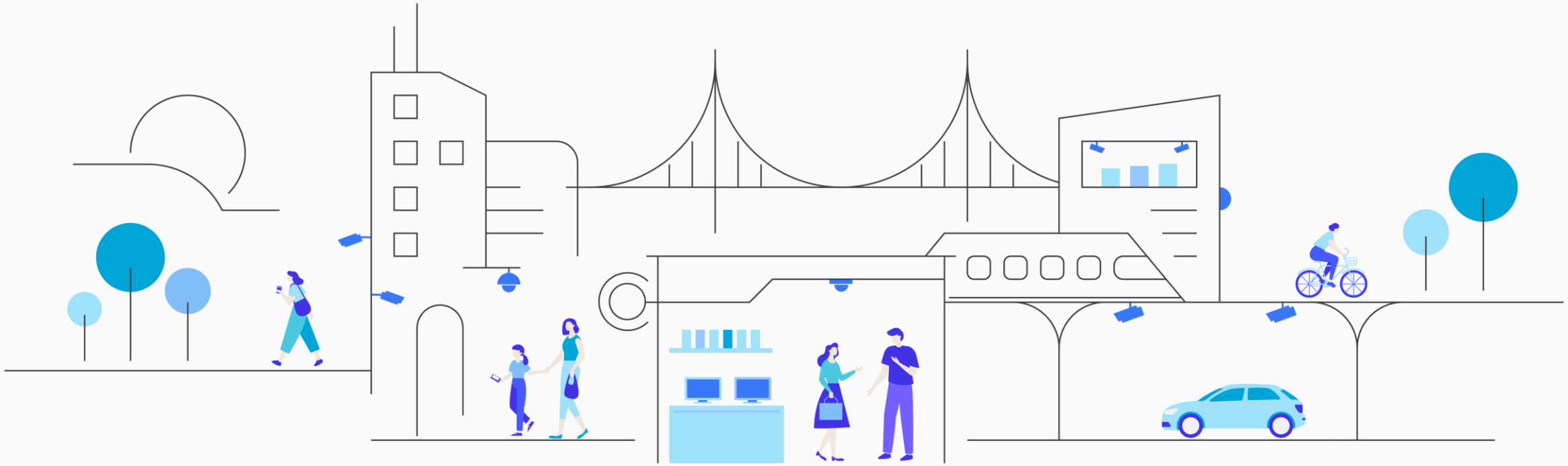
CyberArk特權帳號管理

為了加強對敏感系統和數據的保護，我們即將實施了CyberArk特權帳號管理系統。這個系統有效管理和監控高權限帳號的使用，降低了內部威脅和未經授權訪問的風險。

Mac安全措施

考慮到公司內部Mac設備的使用增加，我們將為Mac系統部署了專門的防毒軟件和數據丟失防護（DLP）解決方案。這確保了所有終端設備，無論是Windows還是Mac，都受到同等級的保護。

Thank You for Your Attention.



VIVOTEK
A Delta Group Company

We Get The Picture