志強國際企業股份有限公司
113 年資安治理運作執行情形

本公司資訊中心下，設置資安部門(資安主管及人員各一名)，每周於部門會議檢討資安政策，並每年提報董事會【本公司於113年12月19日提報董事會】：

1. 詳資通安全Report。
2. 113年執行電腦登入密碼複雜性原則。
3. 113年執行社交工程演練。
4. 資安宣導共3 則 。
5. 113 年尚無發生本公司資訊安全及營運之重大攻擊及洩露資訊事件。
6. 113年集團及海外6廠皆有安排教育訓練，課程名稱：2024年資訊安全宣導。

資通安全 Report

報告者:

資訊中心

Outline

- 資通安全政策
- 硬體安全
- 軟體安全
- 資料安全
- 集團資訊安全分布

資通安全政策

- 資訊安全管理政策
- 資訊系統帳號與密碼管理辦法
- 資訊系統備份還原管理辦法
- 資訊系統變更管理辦法
- 資訊設備維護暨管理辦法
- 資訊網路通訊使用規範及管理辦法
- 資通安全事件通報及應變管理辦法

以上管理辦法收錄於 BPM➔文件管理➔文件庫➔台灣文管中心➔資訊中心

硬體 安全

- ForeSee 行為管理器
  - 應用程式管控、URL管控、上網流量監控
  - 上網權限控管
  - 允許特定網路 port 進出，其餘預設皆為關閉
  - 停用勒索病毒 445 port
- Cisco Fire-Power 防火牆
  - IPS入侵防禦系統、threat、malware defense
  - 允許特定網路 port 進出，其餘預設皆為關閉
  - 停用勒索病毒 445 port
- 核心交換器
  - 網路VLAN劃分、路由區隔
- 郵件系統
  - 郵件傳遞加密、郵件備份半年、紀錄備份一年
  - HA自動化備援機制
- 無線Wi-Fi 系統
  - 內部員工使用
  - 來賓使用(與內網分開)

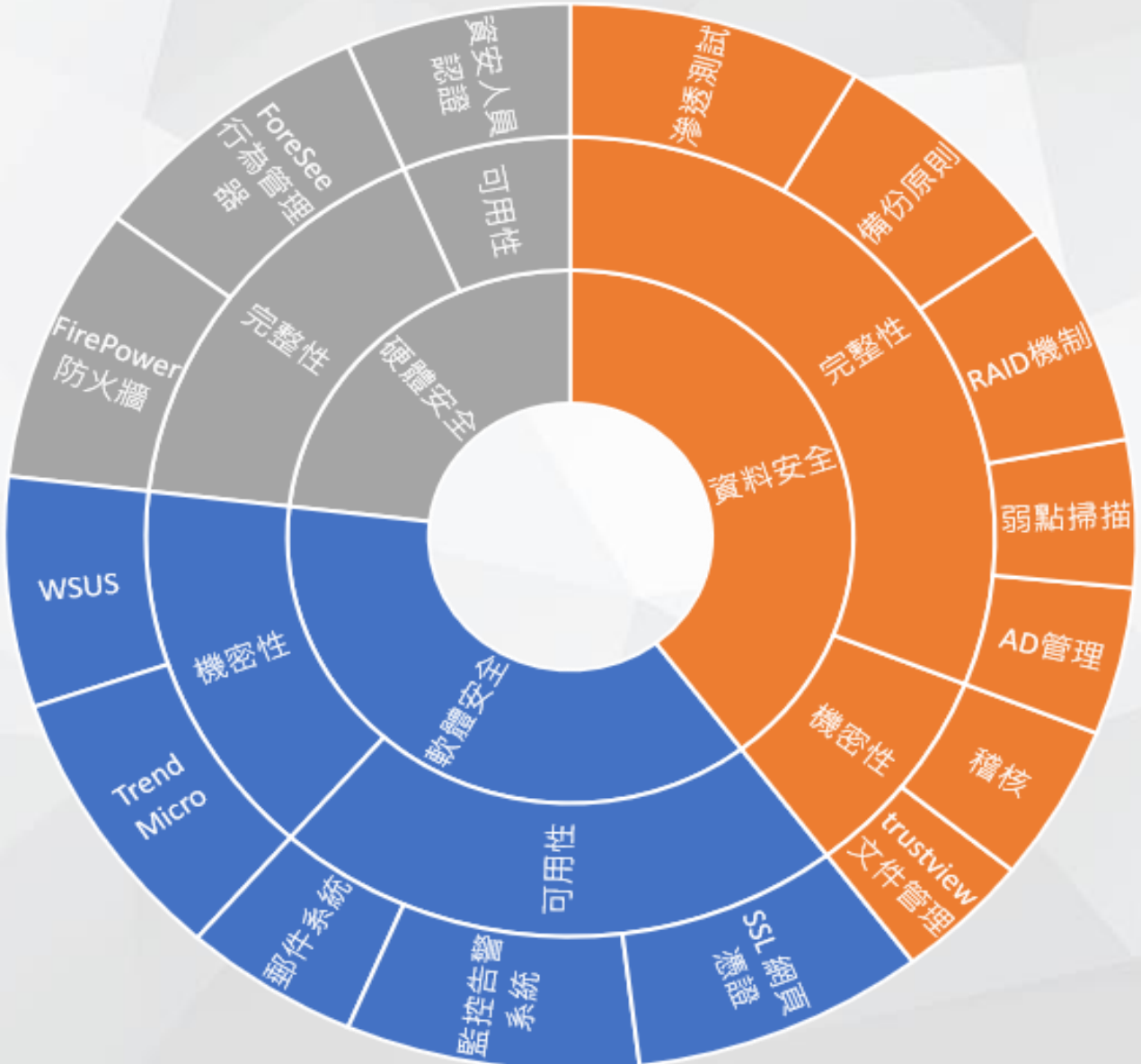
軟體安全

- Windows Services pack Update Services(WSUS)
  - 微軟安全性更新
  - win10/win11共 346支更新
- 防毒軟體 TrendMicro
  - 總電腦數: 3085台
- 集團監控告警系統
  - 主機設備 共209台設備、網路交換器共235台設備
  - 跨國網路監控(MPLS、EZVPN): 共 14條線路
- SSL網頁安全憑證
  - 公司首頁、BPM簽核系統、郵件系統、B2B網站
- Windows Active Directory 管理機制
  - 密碼原則(每90天變更)
  - 網路分享資料夾權限管控
  - USB控管
  - 單一帳號登入管理

資料安全

- 弱點掃描
  - 依稽核需求一年進行初掃+複掃共8次
  - 終端掃描數量超過 24000次
- 滲透測試
  - 每年電子社交工程演練
- 文件加密-Trust view系統
  - 使用於台灣HR、志寧、志雄
- 稽核
  - 品牌客戶稽核(Nike、adidas)、勤業稽核(第三方稽核)、電腦資訊循環 (內部稽核)
- 資訊安全教育訓練
  - 每年一次訓練, 對象為滲透測試上鉤者與年度新人
- 備份原則
  - 系統定時快照(snapshot)
  - 每日差異備份、每周全備份，並依系統特性保留至少四個版本資料
  - 異地備份、磁帶離線備份
- 主機 Server 硬碟容錯 RAID機制
  - 虛擬化主機系統
  - NAS 主機
  - 高可用度企業級存儲裝置

集團資訊安全分布


資安人員認證
ForeSee行為管理器
可用性
FirePower防火牆
完整性
硬體安全
滲透測試
備份原則
RAID機制
弱點掃描
AD管理
稽核
trustview文件管理
SSL憑證
監控告警系統
郵件系統
WSUS
Trend Micro
機密性
軟體安全
可用性
資料安全
完整性
機密性

資安管理範疇

- 每月討論資安管理政策
- 不定期寄送資安宣導信件
- 每年進行電子社交工程演練