資安室報告

Date: 113/05/06

113年第一季 資安報告

報告綱要

- 資訊與網路安全管理團隊
- 風險評估與因應措施
- 安全管理措施
- 資訊安全管理模式
- 資安投資與改善

資訊與網路安全管理團隊

本公司於 111/09/01 起成立資訊安全室，設有專責主管（處協理）及資訊安全專責人員各一名，並由總經理/執行長（原任營運長）擔任資訊與網路安全管理團隊召集人；除資訊安全室外，資訊與網路安全管理團隊包含具專業技術及知識之資訊中心、內部稽核室、人力資源室、法務室及獨立客觀的主管人員（各事業單位及功能單位管理階層），負責統籌、計畫、執行及分析資通安全事件，且每年至少評估一次資通安全政策。

風險評估與因應措施

威健核心資通營運系統	風險評估	因應措施
Email System	1. User帳密被盜,成為垃圾廣告郵名件的發送者 2. 郵件主機被列為黑名單,無法收發郵件 3. Email 主機軟硬體故障的風險	Email System Outsource 採用Office 365 的 Outlook 作為email 的收發, IT 同仁於112年也啟用了2FA的雙重認證, 降低帳密被盜的風險。 email system Outsource也降低了軟硬體故障的風險。
ERP System	1. 營運資訊資料 C,I,A (Confidentiality, Integrity and Availability) 的管控 2. ERP 軟硬體的維運 3. 系統開發維運人員的不足	IT每年會針對ERP使用者的權限請該部門主管覆核,相關採購,銷貨流程也經由Workflow送交相關主管簽署方可放行。 IT部門有計畫的更換ERP DB與AP主機, 並將AP與DB主機虛擬化增加系統使用壽命與韌性。 招募培訓新的IT從業人員,幫助他們加入ERP的開發與維運。

風險評估與因應措施

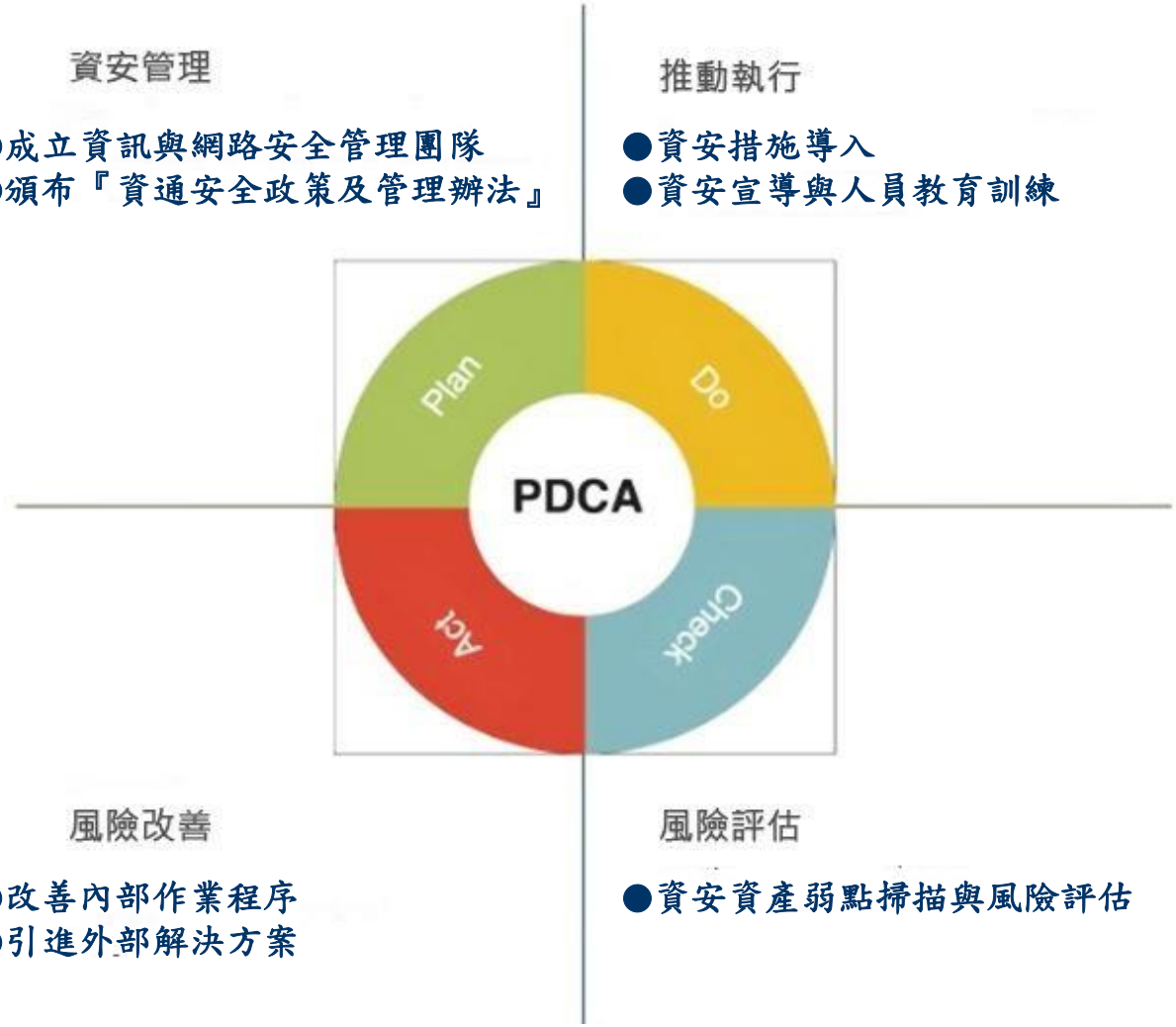
威健核心資通營運系統	風險評估	因應措施
WMS System	1. WMS為自行開發的系統,使用Client/Server的架構,且DB均已虛擬化,故相對於ERP的風險較小較可控 1. 出錯貨(date code)的人為操作風險	WMS主機置於中華電信 IDC 機房,定期更換且WMS Client 在內部網路使用並未暴露於Internet,且使用者須申請安裝 WMS Client端軟體方能存取資料。 庫房人員會對負責揀貨的同仁進行教育訓練。
個資法的遵行	1. 人事系統, 由人事部門管理,並委外維護 2. WKT並無CRM系統或過多的客戶資料對於個資也都採最小資料(僅知原則)保存.故風險相對較小	目前 eHR 系統主機置於中華電信 IDC 機房,並且使用HiNet新世代防火牆服務,故對於來自Internet的風險又多了一份保障。

安全管理措施

管理類別	管理措施	執行項目
權限管理	人員帳號、權限管理與系統操作行為之管理措施	新進員工帳號申請定期覆核有效帳號.離職員工帳號失效。
存取控管	人員存取內外部系統及資料之控制措施	定期覆核使用者系統使用權限
外部威脅	內部系統潛在弱點、中毒管道與防護措施	主機弱點檢測及更新措施 病毒防護與惡意程式偵測基於TWCert的情資分享加強防火牆的設定。
弱點分析	針對PC與伺服器系統弱點掃描與檢查、修補措施	定期檢查與修復高風險的弱點.若無法修復將提醒系統管理者注意該風險。
社交工程與資安教育訓練	針對使用者同仁定期宣導資安觀念 (email與新人訓練)	IT與IS部門不定期發email宣導分享資安新聞於新人訓練時派員講述威健資安相關議題與措施。

資訊安全管理模式

採用PDCA 循環流程管理模式，確保資訊安全管理目標之達成並且持續改善。



資訊安全管理模式

資安管理 (Plan)

- **成立資訊與網路安全管理團隊**

  本公司於 111/09/01 起成立資訊安全室，設有專責主管（處協理）及資訊安全專責人員各一名，並由總經理/執行長擔任資訊與網路安全管理團隊召集人；除資訊安全室外，資訊與網路安全管理團隊包含具專業技術及知識之資訊中心、內部稽核室、人力資源室、法務室及獨立客觀的主管人員（各事業單位及功能單位管理階層），負責統籌、計畫、執行及分析資通安全事件，每年至少評估一次資通安全政策。

- **頒布『資通安全政策及管理辦法』**

  資通安全政策制定及評估
  資通安全組織及權責
  資訊資產分類與控管
  人員安全管理
  實體及環境安全管理
  通訊與作業管理
  存取控制
  系統開發與維護
  營運持續管理
  資通安全措施符合性之檢核

資訊安全管理模式

推動執行 (Do)

- **資安措施導入**

Email 上雲,採用O365 mail並使用中華數位的mail spam server攔截過濾垃圾郵件與威脅郵件成果良好. 113年正常郵件(113/01/01~113/03/31)：正常郵件: 2,592,595封, 垃圾郵件:126,506封, 威脅郵件:41,665封攔截精準度：99.84% (統計自 113/01/01 ~ 113/03/31)。

- **資安宣導與人員教育訓練**

資安宣導: MIS 每月定期email宣導. 資安室收集資安情資,不定期email宣導. (up to 113/03/31 Total 宣導次數: 8次)。
金管會表示，為強化上市櫃公司資安監理，今年(113)首季將修訂重大訊息問答集，明確規範資安事件的「重大性」標準，當公司核心資通系統遭入侵以致無法提供服務，即必須重訊揭露。

資安教育: MIS/CIS(資安室)於新人訓練時針對駭客,病毒,網路釣魚,電腦蠕蟲,社交工程,密碼維護等議題,提出說明與宣導。

資訊安全管理模式

風險評估 (Check)

- **資安資產弱點掃描與風險評估**

  IT人員每年定期對提供internet上服務的主機 (ex: Web Server, DNS Server, eHR Server...)進行弱點掃描. 針對有重大風險的主機進行更新版本. 若因服務主機無法更新, 將提醒管理者注意或做其他控管。
  此外若 TWCert 針對資安情資有重大風險通知時, IT/IS部門會依據所提供的資訊加強防護。

風險改善 (Action)

- **改善內部作業程序**

  IT人員於 113/01發現有同仁在未告知MIS同仁的情況下私自在公司內部網路接入一無線 AP,後經 IT人員查找發現並斷接該無線 AP. 考量此一事故,有可能造成資安風險,故請稽核修改補強 "資通安全政策及管理辦法"。

- **引進外部解決方案**

  防毒中控台上雲, 將防毒軟體F-Secure更新為WithSecure, 一來將防毒中控台上雲, 另一方面將部分使用者導入EDR防護, 提升防毒防駭功能

資安投資與改善

- 資安事件與因應:

  駭客病毒入侵: 113年第一季無重大駭客或病毒入侵事件.
  電腦網路故障: 113年第一季無重大網路中斷事件。
  環境設施故障: 113年第一季無重大環境設施(泛指機房冷氣,供電等設施)故障.
  重大資安事件: 113年第一季無因發生重大資通安全事件所遭受之損失或影響營運、商譽等之情事.
  113年第一季無經證實侵犯客戶隱私或遺失客戶資料投訴之情事.

- 資安投資與改善:

  113/03 IT部門更換ERP資料庫主機，以提高硬體保固和硬體效能。
  113/03 IT部門更新防毒軟體F-Secure到新的WithSecure, 一來將防毒中控台上雲, 另一方面將部分使用者導入EDR防護, 提升防毒防駭功能。

- 113年第一季 資安人員相關教育課程與活動:

  本期無參與資安人員相關教育課程。