2025 年度資訊安全執行成果

(一) 114年度召開4次資安委員會議(3/20、6/19、9/25、12/11)，檢討各單位資安政策之執行情形。

(二) 配合集團資安查核及交流

1.中鋼集團工控(OT)資安訪查，中鋼 Y6於6/19日至冷軋廠與設備安全組人員進行114年 OT 資安訪談會議，訪談重點摘要如下:

(1)中鴻目前使用 VPN 遠端存取 L1 製程資料，Y6 分享使用製程資訊管理系統(SPC)收集製程資訊的作法，使用者再連線 SPC，無須直接存取 L1 系統也可獲取必要資訊。

(2)針對廠商的技師須從國外遠端連線處理 L1 系統，中鴻廠內會有同仁為求作業便利，直接利用手機 wifi 直接連外。Y6 建議可在電腦上安裝白名單軟體，管控可執行程式，杜絕惡意程式。另外，Y6 建議此類遠端連線需求都要透過 VPN，目前中鴻已將調機筆電之 BIOS 中 wifi 功能停用(disable)並設管理者密碼，欲使用須簽核廠長核准。

2.參與中鋼集團資安聯防會議(3/20、6/26、9/19、12/18)。

3.8/20進行中鋼集團公司年度資安交流，中鋼總評如下：

(1)參考上市上櫃公司資通安全管控指引新增之第二十五條項目，建議清查外部人員可視之電子看板設備，並強化管理機制。

A.已於 11 月底完成全公司電子看板設備清查。

(2)SSC (SecurityScorecard 資安評級)分數截至訪查當天為 89 分，符合標準(80分)。另於 12/8 再次檢視，分數已提升至 90 分。

(三) 12/03完成 ISMS 第二年度外部稽核作業，整體審查順利，未發現不符合事項，現行資訊安全管理系統運作符合 ISO 27001標準要求，證書持續有效。

(四) 資訊安全及時防護

1.與中華資安簽訂委外監控服務專案(MDR 與 SOC)資安服務合約，透過監控與即時通報資訊安全事件，協助公司處理資安事件、縮短應變時間與控制資安事件災損範圍，並提供月報、季報，找出隱藏的資安危機。

2.與中華資安簽訂委外監控 HiNet WAF (網站應用防火牆)資安服務合約，透過電信等級的網站防護設備專責分析網站訊務內容，阻擋已揭露之攻擊行為，並可針對零時差攻擊即時回應並阻擋，另提供日報、月報供查閱。

3.導入 IPMAC 管制方案建置，透過此軟體可有效控管非法設備，落實連網裝置識別盤點，讓網路及資訊安全管理者充分掌握 IP 使用狀況。

4.導入資料庫稽核軟體 Imperva DAM，藉此可取得完整的資料庫活動細節，留存存取資料庫的行為軌跡，產出自動化與集中化的資料庫稽核與報告，以符合 ISO

27001對於資料庫的稽核要求。

5.勤業眾信電腦審計查核發現,下列系統未設置適當之密碼原則,已要求調整為:帳號鎖定閾值:5次;帳號鎖定期間:15分鐘。

(1)Active Directory（AD）

於114/06/20完成帳號鎖定政策調整,將帳號鎖定閾值設定為5次,符合密碼原則要求,改善完成。

(2)資料庫主機（DB Server／AIX 7.2）

因 AIX 系統安全機制較為嚴謹,僅支援連續登入失敗達一定次數即進行帳號鎖定,無自動解除鎖定功能,需由系統管理員人工予以解鎖。114/06/24已完成帳號鎖定閾值5次之設定,改善完成。

(五) 114年度共執行46台主機弱點掃描、行動應用平台網頁弱點掃描及公司官網與電子商務平台滲透測試。相關作業已於114年1月完成初次檢測,並依檢測結果提出之改善建議逐項進行修正,後於114年5月完成複測,所有弱點項目均已改善並符合安全要求。

(六) 114 年釣魚郵件實測結果及統計

1.受測總人數624,點擊連結或開啟附件人數59,比率9.64%。

2.今年受測結果高風險之59位同仁將安排參加明年度 A11辦理之資安訓練。

(七) 114年資訊安全查核實際執行情形:

1.114年文書個人電腦軟體查核結果,經過濾及比對文書個人電腦軟硬體帳目資料後,各單位並無安裝非法版權 BSA 會員軟體之情形發生。

2.每月進行文書用(OA)個人電腦長時間未關機查核。

3.每月進行個人電腦防毒軟體阻絕資安威脅查核。查核結果皆已被防毒軟體阻絕,無資安情事發生。

4.每季進行使用 USB 外接儲存設備進行檔案存取查核。目前申請使用 USB 的比率管制為20%。

5.每季進行具有安裝軟體權限之個人電腦安裝軟體查核。

6.每年進行文書用個人電腦雲端硬碟使用重新申請。

7.每年進行個人電腦 USB 埠連接手機裝置重新申請。

(八) 114年資安教育訓練與資安宣導執行情形:

1.新進人員到職訓練將資安宣導列入(含資安政策):建立資安宣導資料

(1)參考行政院公告之新進人員資安宣導範本研擬草案,經提報 111/3/10 本會議決議,通過「新進人員資安宣導單」,列入人事課新進人員訓練宣導與簽署留存文件之一。

(2)持續同步由承攬商對其新進人員依宣導單展開宣導,截至 114/11/20 止承攬

商計 360 人完成簽署(較 114/5/20 止 341 人)增加 19 人)。

2.定期每月 ERP 佈告欄資訊安全宣導(資料來源：數位發展部資通安全署、中鋼資源、中鴻 A3…等)

ERP 佈告欄資訊安全宣導(數位發展部資通安全署授權獲獎宣傳海報)：

(1)114/8/7 宣導「掃著爽快等著重灌」及「中鋼資訊安全委員會 114 年 6 月資安宣導」

(2)114/8/7 宣導「網路通訊停看聽」及「中鋼資訊安全委員會 114 年 7 月資安宣導」

(3)114/9/5 宣導「不要輕易接受請求，不是每個都是好友」及「中鋼資訊安全委員會 114 年 8 月資安宣導」

(4)114/10/29 宣導「不給錢就鎖檔，小心網路勒索陷阱」及「中鋼資訊安全委員會 114 年 9 月資安宣導」

(5)114/10/29 宣導「網路誘惑多危機 資訊安全要小心」及「中鋼資訊安全委員會 114 年 10 月資安宣導」

(6)114/11/27 宣導「騙面之詞，你敢信？」及「中鋼資訊安全委員會 114 年 11 月資安宣導」

3.不定期資訊安全教育訓練(中鋼資源、納入年度教育訓練計畫規劃…等)

(1)114 年「資訊安全認知訓練」，對象為各單位派訓人員，分上下半年各辦理 1 場次，由中華電信訓練學院高雄所蔡旻芳培訓師擔任講師，上半年場次於 5/16(五)、下半年場次於 7/16(三)辦理完成。

(2)114 年「資訊安全宣導教育訓練」，對象為資訊安全委員會與會成員，於例會中進行 1 小時訓練，分別為第 1 季 3/20(四)、第 2 季 6/19(四)、第 4 季 12/11(四)開課。