|  |  |  |
| --- | --- | --- |
| 考評人員簽章： | 權責主管： | |
|  | |  |

附件3

新進人員心得報告

部門：資訊室

期間：110年7月5日 至 110年8月4日

|  |  |  |
| --- | --- | --- |
| 報告人姓名 | 指導人評語及簽章 | 主管評分及核章 |
|  |  |  |

註：新進人員繳交心得報告一份給指導人，撰寫之心得報告應包含工作內容、心得感想、對個人與公司展望及建議等項，以WORD橫式16號字標楷體書寫並標註頁次，由指導人及主管核閱評分後送人資部門。

附件3-1

**探採事業部新進人員訓練 (含試用或實習）心得表**

110年 7月 6日

|  |
| --- |
| 實習心得  一、關於工作內容的初步了解  跟其他注儲組的人不同，我除了報到第一天到通霄報到之外，其他時  間皆在苗栗市的資訊室實習，原先還沒有進公司以前，我不大知道探採注儲的意思，經過部門內前輩的介紹，才知道原來是將在南部天然氣廠的氣體導到地底儲存，在地底運送至目的地後，供給北部用戶需求，因為我的家鄉在高雄市，中油的楠梓煉油廠以及大林蒲附近的廠區對於我而言，都不算陌生，不過也僅有煉油廠這個概念，直到我真正踏入通宵的廠區，看到球槽等這些大型的設施，才讓我真正感覺到離石油生產這個概念如此的接近，整個廠區的分工以及組織編制也十分的細微以及嚴謹，在和處長聊過相關的工作內容後，我發現資訊安全是我往後需要著重的工作方向，OT這個概念對於我而言是很陌生的，之前我只有接觸過IT這個名詞，後來找資料後才了解兩者的不同，許多企業在推動資安防護的工作上，都會參考ISO 27001的要求，而在OT領域，則是依據IEC 62443的標準，在數位轉型的風潮之下，為了因應各種資料交換與分析的需求，IT（資訊科技）與OT（營運科技）環境的融合已成必然的趨勢，但這也打破了過往OT環境的網路實體隔離，減少了一些保護，再加上OT環境的設備往往採用相對老舊的作業系統平臺，不僅存在著許多漏洞，而且因為需要持續運作，即使有對應的修補程式與軟體、韌體的更新版本，也不易找到合適的空檔來套用，結果導致OT環境面臨極大的資安風險，中油公司是一家歷史悠久 |

|  |
| --- |
| 的能源企業，可以想見內部的資訊系統已沿用已久，若要做出調整以及變動，可能都需要花費不少的人力以及物力，近年來，資訊安全一直是企業發展的一大重點，越是自動化的系統，暴露在風險下的機率就越高，在得知未來工作的相關內容後，因為之前從未接觸過相關的議題，所以覺得有些無法想像工作的模式以及預期的成果，不過一想到可以學習到許多之前不曾接觸過的東西，我也覺得很期待，也希望自己能在實習期間好好學習，並且快速進入工作狀態，來資訊室實習後，發現學姊需要執行許多部門的資安稽核作業，這是需要有專業證照才能勝任的，也希望未來自己能有機會順利考取iso27001資訊管理系統主導稽核員認證。  二、實際參與的採購案例  做為新人，組長先請組內的學長帶著我們做一些簡單的採購案，分別是  VM Essential Kit版權購買以及Windows Server 2019版權購買，這兩個案例都是共契的類型，因為過程比較單純，作為新手練習正合適，對於共契這個概念我也是第一次接觸到。  共契意思是指一機關為二以上機關具有共通需求特性之財物或勞務與廠商簽訂契約，使該機關及其他適用機關均得利用該共同供應契約辦理採購。對於廠商而言，與訂約機關簽訂共同供應契約後，即有義務依約供應採購標的予該契約之所有適用機關，有此可見，共契類型的品項有固定的契約模板可以使用，也不必經過公開招標的過程。  至於採購分為兩類，分別是財物以及勞務，相較於財物，勞務因為牽涉到許多人員證照的問題，所以複雜許多，前段所提的兩個採購案都是單純財物分類的案例，因此只需要考慮到產品規格的問題，這也是我認為整個過程最複雜的地方，軟體更新還必須考慮到向下延伸性的問題，以Windows Server 2019 為例，2016以及2012R2都能就地升級至2019版本，  因此可以透過直接向微軟買授權金鑰直接升級，微軟也提供不同的套件方案供使用者作選擇，如何針對部門內部機台的情形，選擇最有利的方案，是採購者必須深入去了解的，我覺得一個好的決策，不但必須考慮到改善現狀的方法最好還要能夠思考到未來是否可以針對既有規格，彈性的作變動。  透過多方面的蒐集資料以及詢問，我也發現共企提供的類型有一定的限制，若想照著這種模式進行，就必須照著上面所提的產品規格作購買，比如windows server 所提供的類型為datacenter 若想要選擇 standard的版本，可能就不能選擇這種模式，我覺得共企採購提供了一個公平的模式，採購者可以在價格受保障的前提下，評估自己需要的數量，向廠商下標，除此之外，與廠商所簽訂的合約中還能夠附加小於十萬元的商品服務，這點可以由買賣雙方自由運用，這也給制式的共企採購帶來些許彈性空間， 雖然說共企採購省下了許多招標定價，以及擬定合約等等複雜的過程，但若部門需求較為特殊，謹慎評估後也不一定皆須走共企模式，我想契約應該如何簽訂，以及如何做有效率的購買，真的是需要經驗的累積，才能很快從大量的訊息中，找到方向，雖然目前主要還是學長在處理整個採購案，我們只是從旁見習，不過至少對於採購的流程以及知識有些許的概念。  三、資訊安全專法以及知識  到了資訊室以後，我深深的體會到資訊安全是整個資訊業務中，相當重要的一環，每年每個員工都需要上三小時的資安課程，電腦設備也會定時進入鎖定的狀態，我覺得這應該是目前企業的常態，資訊安全防護的種類很多，我們也都做到基本的規格，學姊在向我們上課時有以瑞士奶酪理論  (附圖一)來向我們闡述資安事件的發生就如同這個示意圖般，見微知著  瑞士乳酪理論(Swiss Cheese Model) | olofsdesign      附圖一: 瑞士乳酪理論示意圖  ，如附圖一所示，假設我們電腦的防護就如同乳酪般，雖然我們做到層層的防護，不過若中間皆存在一些小漏洞，攻擊便可突破防護層，侵害我們的電腦本身，電腦駭客的攻擊手法一直更新，似乎是防不勝防，尤其是社交工程攻擊，更是充斥在我們的日常生活中，我覺得日常的釣魚信件演練是很重要的，這會時時提醒我們提高警覺性，避免遇到攻擊時，毫無危機意識，平常我們就必須保持備份重要資料的習慣，下班時要記得關機，並隨手拔掉網路線，做好我們能做到的基礎防護。  雖然我們公司不算是傳統的公務機關，不過我們公司歸屬在關鍵基礎設施提供者的類別裡，所以也適用資通安全管理法，裡面有相當多的規範，其中也包括事發當下要儘快通報這一點，我覺得這一點十分的重要，在錯誤發生時人們往往想著該如何快速彌補，只是我們往往羞於讓別人知道自己的狀況，而造成延誤通報的後果，現今的電腦病毒往往攻擊單機後會隨著網路系統快速蔓延至其他電腦，有的還會藏在快取記憶體中，關機也不 |

|  |
| --- |
| 能確保完全隔離病毒，所以若發生資安事件後，能夠越快啟動補救措施，儘快向上級通報，使大部分人趕緊了解狀況，才是最有效率的補救方法。  近幾年來，勒索病毒日益猖狂，軟體變種的速度更是大幅攀升，聽部門裡資深前輩的分享，才了解當時勒索病毒事態所造成的嚴重衝擊，技術支援組的同仁，連續幾個月都在處理電腦重灌的問題，連坐下來喘口氣的時間都沒有，當時我只有在新聞裡看見這則事件的報導，也覺得事態很嚴重，心想如此龐大的國營企業，竟然會成為駭客的攻擊目標，後來我看過許多網路專題的講解，才了解到這是一次預謀許久的攻擊事件，勒索軟體其實早就潛伏在企業網路裡部署，等時間到了再同時發動，讓破壞效果更大，而病毒入侵的途徑也相當複雜，有可能是員工不小心點選了釣魚郵件、有可能是遭感染的USB被插入公司電腦、也可能是駭客透過軟體漏洞植入惡意程式。在順利進入企業內網後，駭客會試圖破解AD（網域控制伺服器）或者具備派送功能的資產管理軟體權限，將病毒擴散到轄下的各台電腦後伺機潛伏。  附圖二:近年勒索病毒攻擊事件統計 |

|  |
| --- |
| 根據附圖二所顯示的資訊，我們可以發現經由電子郵件附件或惡意網站入侵企業的勒索病毒近年來已大幅減少，不過若我們從媒體報導來看，許多人會覺得網路上的勒索病毒數量似乎並未減少。這個現象背後的原因是因為近年來勒索病毒集團對於攻擊目標的篩選更加嚴格。他們開始放棄亂槍打鳥的大規模勒索病毒垃圾郵件攻擊，而改用一種專挑大型獵物的攻擊手法。換句話說，勒索病毒集團現在對於家用個人電腦 (小型獵物) 比較不感興趣，取而代之的是中大型企業 (大型獵物)。勒索病毒集團之所以這麼做，原因是他們覺得將火力集中在這些大型獵物可以提高獲利。  由此可知，面對未來攻擊型態轉變的趨勢，中油公司勢必面臨更艱鉅的挑戰， 尤其是製造業還必須牽涉到OT架構等嚴峻的問題，若網路分段有漏洞，未來駭客可能會先入侵 IT 網路然後再轉移到 OT 網路。另一個可能的問題是 OT 網路含有安全性不足或企業未確實掌握的遠端直接連線。在遭遇勒索病毒事件過後，企業的善後工作不光只有讓生產線或業務恢復營運而已，還必須將一開始導致勒索病毒感染的資安弱點徹底解決。  這個月有個機會，可以和學姊一同回到注儲組，參與資安健檢的事宜，  廠商會針對我們提出的網路架構圖，提出需要改善的地方，並會幫我們的伺服器偵測封包等等，因為注儲組為生產單位，所以會有OT網路方面的問題，期間有和注產組的學長聊到，IT還有OT的網路是有區分開的，而且OT是存在一個封閉的網域中，較為安全，不過也是必須避免橫向感染的風險，廠商會針對評估的情形，向我們提出改善的建議，這個資安健檢每年需要一次，委託給廠商幫我們作檢查，我認為資安方面我們能做到的  就是事先的預防以及萬一發生問題，應該如何快速補救，面對瞬息萬變的  攻擊型態，我們也只能夠將我們能夠處理的部分先作好，平時就要養成良 |

|  |
| --- |
| 好的習慣，我想稽核絕對不是為了應付每年的抽檢才需要作的流程，畢竟資訊攻擊的型態以及方式我們並不能在第一時間完全掌握，每年的檢測也能讓我們了解目前資安方面的現況，幫助我們評估是否需要在架構上作更新。  四、注儲組工控系統(ICS)概念理解    附圖三:工業控制系統示意圖  **工業控制系統 (ICS)(如附圖三)**是多種控制系統與設備的總稱，包括了工業流程運作及自動化所用到的各類裝置、系統、網路及控制器。視產業而定，不同的 ICS 會有不同的功能，但其目的都是要透過電子方式來有效管理工廠作業。今日，ICS 裝置和通訊協定幾乎遍及了每一個產業與關鍵基礎設施，例如：製造、交通運輸、能源、水處理等產業。注儲工程處的設施包括DCS，PLC，還有人機介面系統等等，包含一台電腦為中控中 |

|  |
| --- |
| 心，其餘的電腦皆為操作者電腦(只能觀看數據，不能下指令)，這也是我第一次接觸到工控的概念，以往接觸到的皆為IT系統方面的業務，所以對DCS還有PLC這些概念是很陌生的，工廠端的生產模式，紀律嚴謹，責任也區分的很清晰，注儲處的ICS系統分工大致如下，DCS為分散式控制系統，在 DCS 中，PLC 則是用來當成整個監控作業的現場控制器，所有PLC的資料會一起匯集在DCS中，再由DCS上的通訊點將資訊送去外站，而系統也分為三個工作站，AP(應用工作站)，PP(規劃工作站)，OP(操作工作站)，其中PP是可以寫程式來控制DCS的，只有一台，而OP有好幾台，可以看到PP上的資訊，但不可以做任何更改的動作，至於AP是用來傳輸PLC的資料到DCS，並且會透過兩次的OPC(定義格式)，將資料改成DCS接收的格式，還包括一個診斷系統，這些PLC還有DCS的機台都十分龐大，線路也十分複雜，若要所有機台的IP資訊彙整好，並且將整個網路架構圖整理出來，是十分浩大的工程，注儲處的學長也還在構思中，這些設備若是需要維修或是更換程式，都需要交給廠商來評估， 我覺得要完全了解DCS整套系統運作細節包括PLC程式碼的部分，不但需要自身的努力學習，經驗以及他人的指點都是不可或缺的，聽學長說，有的資深的前輩可以自己去修改PLC的程式，使用起來還十分熟練，想必是多年來累積的經驗以及功夫使然， |

|  |
| --- |
|  |

|  |
| --- |
|  |

|  |
| --- |
|  |

附件4

台灣中油股份有限公司

新進人員面談紀錄表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 部門 | | 姓名 | | 員工編號 |
|  | |  | |  |
| 面談日期： | | 年 月 日 | | |
| 面談事由及紀要： | | | | |
| 後續處理方式： | | | | |
| 參加面談人員簽章： | | | | |
| 新進人員 | 指導人 | | 權責主管 | |
|  |  | |  | |

附件5

|  |  |  |  |
| --- | --- | --- | --- |
| 台灣中油股份有限公司  新進人員綜合考核表 | | | |
| 部門 | 姓名 | | 員工編號 |
|  |  | |  |
| 訓練(含試用、實習)階段 | | 原始分數 | 說明 |
| 第一個月考核成績（A） | |  | 各單位如已依不同及格標準核給分數者，應自行調整改以80分為及格分數。 |
| 第二個月考核成績（B） | |  |  |
| 第三個月考核成績（C） | |  |  |
| 第四個月考核成績（D） | |  |  |
| 第五個月考核成績（E） | |  |  |
| 第六個月考核成績（F） | |  |  |
| 平均成績（(A+B+C+D+E+F)/6） | |  |  |
| 增減分 | |  | 由權責主管就新進人員表現予以增減分，以不超過5分為原則。 |
| 總成績（平均成績+增減分） | |  |  |
| 考評人員簽章： | | 權責主管： | |