廉政案例宣導(3)：詐領加班費案，切勿因小失案

一、姚○○係臺北市政府捷運工程局機電系統工程處副工程司兼主任，為依法令服務於國家所屬機關而具有法定職務權限之公務員，竟意圖為自己不法之所有，於民國 103 年 8 月至 11 月間，明知未實際加班，竟仍申報加班及請領加班費，復將加班申請單及免刷卡加班簽到退紀錄表層轉不知情之單位同仁，使人事、會計人員陷於錯誤，如數撥付姚○○溢報之加班費至其薪資帳戶內，姚○○以前揭方式前後總計詐得新臺幣 2 萬 7，270 元。

二、案經法務部廉政署調查後認事證明確，移送臺灣臺北地方法院檢察署偵辦，業經檢察官偵查終結，依貪污治罪條例利用職務機會詐取財物罪提起公訴。

（本文摘錄自法務部廉政署新聞稿）

工作效率與資訊安全間的兩難

◎魯明德（作者為科技大學資訊管理系講師）

適當利用硬體驗證機制及管理規範，時時落實稽核，才能維護資訊安全。

由於平板電腦及智慧型手機越來越普及，且功能越來越強大，很多企業剛開始為方便高階主管出差在外，處理公事不便，而開放高階主管可以使用手持式裝置登入公司電腦，以免耽誤公事；漸漸地，這股需求已經蔓延到員工了。公司的業務人員因為需要長期在外，常常乘著空檔利用自己的電腦就把工作完成，等回公司再複製到公司的電腦，導致公司的電腦常因此而中毒。在資訊部門工作的小潘，接到長官指示，要他研議如何提升公司的資訊安全。

小潘心想：如果把電腦的 USB 介面都封起來，不就可以解決了嗎？但是，資訊部門的工作應該不是防弊，而是積極興利才是；業務人員利用工作空檔整理資料，等回公司再複製到公司的電腦，可以提升工作效率，資訊人員要防止的應該是危安事件才是。

利用師生下午茶約會的時間，小潘把這個問題提出來跟司馬特老師討論，司馬特老師喝口咖啡後娓娓道來，讓員工使用自己熟悉的設備，是可以提高工作效率，且對企業主而言，還可以節省軟硬體設備的支出，以及另外花費時間和金錢安排教育訓練；但是，相對地也隱藏了一系列企業資料外洩與安全性的問題。

根據國際電腦安全協會報告：60%的洩密事件，是來自企業內部，只有15%是來自外部入侵；表示企業對於自己內部資訊機密的保護作為，還不是很周全。商業管理協會的研究報告也指出：白領工作者平均每週處理11份機密營業文件，而且這些機密文件常常會在不必要的情況下曝光。另外，39%的工作者曾經將客戶資料寄出公司；52%的員工曾在離職時，將工作資料帶走；86%的員工坦承習慣性將郵件轉寄其他人；26%的員工甚至會使用免費信箱寄送工作資料。由以上的研究發現：企業的危安事件大部分來自內部。

以往企業對於資料外洩防護所做的資訊安全措施，不外乎是：檔案加密、可移除式媒體控管及網路監控。採用檔案加密的方式，需要額外的軟、硬體配合，初期有建置成本，執行中有維護成本。也有企業採用可移除式媒體控管的方式，它的主要做法是：要求人員出入辦公場所時，交出手機，或是在電腦的USB介面上貼封條,並由中央控管所有終端電腦的儲存裝置，需特定人士核准才能使用。此舉不但不夠人性化，還會造成工作上諸多不便。至於透過側錄、監控、記錄，或限制藉由網路流通的未加密文件檔案的方式，如E-mail、Skype、http、ftp等作業，防範機密文件透過網路而外洩的方式，除不夠人性外，這些管制行為，通常無實質控管功效，僅能在事後稽核時產生作用。

聽完司馬特老師的說明，小潘又問道：現在手持式裝置的功能強大，又可提升工作效率，應該如何管理才好呢？司馬特老師喝口咖啡繼續說：由於智慧手持裝置的規格接近PC，包括大容量的儲存能力、各式各樣的應用軟體等，許多PC可能遭受的攻擊，包括詐騙網站、惡意軟體，一樣可能透過這些智慧手持裝置而入侵企業內部。此外，由於智慧手持裝置的體積小，又容易攜帶，遺失或失竊的風險大增，存放其中的客戶資料、公司機密或財務資訊，可能就會因此外流。

但由於它可以讓員工利用瑣碎的時間處理公事，提升工作效率，禁止或開放對企業而言是個兩難的問題。日本的 NTT 調查發現，超過 50%以上的員工會自行攜帶智慧型手機上班，但只有 20%左右是真正得到企業正式同意，顯示員工真的有此需求。

對於資訊安全的管理，應該是從需求面去疏導而不是一味地防堵。在硬體上，可以透過雲端服務、加密通信網路及多重身分驗證等機制，讓員工即使是使用自己的私人設備，也不會讓企業的重要資訊留存在裝置上，如此一來，如果員工的手持式裝置遺失或失竊，也不會造成企業的機密或客戶的資料外流，從而維護資料的安全。在管理上，也要訂定使用規範，讓員工知道自己的權利與義務，並時時稽核。唯有落實管理制度，才能維持資訊的安全。

摘錄自清流月刊

反暴力恐怖攻擊常識(1)

（摘錄自內政部警政署反暴力恐怖攻擊常識彙編）

壹、基本認識篇

一、恐怖攻擊是什麼？

「**恐怖攻擊**」係指個人或組織基於政治、宗教、種族、思想或其他特定之信念，意圖使公眾心生畏懼，而從事計畫性或組織性之重大犯罪行為。

實施恐怖攻擊或參加、資助恐怖組織之人員稱為「**恐怖分子**」。

恐怖分子在三人以上，有內部管理結構，以從事恐怖行動為宗旨則稱「**恐怖組織**」。

恐怖攻擊及一般暴力均屬犯罪行為，但二者仍有差異如下：

(一)動機及目的

1. 暴力犯罪：大多肇因於獲取財產利益、報仇、人格（精神）異常，

著重遂行非法行為。

2. 恐怖攻擊：為實現政治、宗教、種族、思想或其他特定之理念，以非法手段向公眾散播恐怖意象。

(二)目標

1. 暴力犯罪：針對特定對象。

2. 恐怖攻擊：攻擊一般民眾生命或財產。

(三)手法

1. 暴力犯罪：一般犯罪手法。

2. 恐怖攻擊：手法較超乎常理。

(四)武器

1. 暴力犯罪：大多使用常規武器。

2. 恐怖攻擊：除常規武器外，不排除使用毒性化學物質、生物或放射性物質等，甚至以汽車、人身、航空器作為攻擊武器。

二、如何識別可疑人物？

(一)刻意靠近重要人士，且堅持親交不明物品。

(二)面露驚慌、言語支吾、偽裝鎮靜。

(三)表現詭異、催促檢查或態度蠻橫、不願接受檢查。

(四)偽稱熟人、無端獻殷勤。

(五)打探警衛輪班時間或監視器拍攝角度、內容者。

(六)身分不明，持用數張不同身分證件，攜行物品不符其身分及行動目的。

(七)持有重要人士行程、藍圖、逃生疏散計畫、密碼等資料。

(八)刻意喬裝，著裝明顯不符其身分或季節。

(九)衣服異常突起或特別寬鬆。

(十)無故逗留敏感地區，頻繁出入管制區域、廁所、公用電話亭，窺視犯罪現場、客機坪、警衛輪哨情形，對水電系統及政府機關記錄（繪圖、攝錄影、默記）。

(十一)不斷造訪同一個重要地標並對它攝（錄）影。

(十二)用步伐數來計算各個出入口、警衛崗哨、監視攝影器之間的距離。

(十三)無故棄置攜帶物品潛逃。

(十四)已過安全檢查時間，卻匆忙趕到檢查現場，以時間不及為由，欲

強行入場。

(十五)來自恐怖活動頻繁之地區。

(十六)攀爬或剪斷電力、供水、政府機關或重要象徵建築物周遭圍籬。

(十七)向供水設施或飲用水槽傾倒物質。

(十八)將不明或未標記之車輛停放在電力、供水、政府機關或重要象徵建築物周遭。

(十九)開啟或破壞人孔蓋、消防栓、建築或設備。

三、如何識別可疑物品？

(一)接獲通報應注意檢查之物品。

(二)重要目標附近無人認領或來歷不明之物品。

(三)經過偽裝之物品。

(四)攜帶不符職業、季節之物品，或實際用途與攜帶目的不相符之物品。

(五)無端改變位置、形狀、大小之固有物品。

(六)發出異常氣味、聲響之物品。

四、如何識別可疑車輛？

(一)車籍不明或未標記，車牌前後不一，缺少進入管制區之車證，車證被偽（變）造或不符規定。

(二)車體結合部位及邊角外沿的車漆顏色，與車身顏色不一致。

(三)曾改變顏色。

(四)車門鎖、行李廂、車窗等有被撬開痕跡，車燈破損。

(五)車體外露怪異導線或細繩，或駕駛座旁有額外電池裝置。

(六)行李極少，車輛卻異常沉重。

(七)貼上大片反光貼紙或加裝窗簾，完全看不見內部。

(八)違規停留、繞行於重要基礎設施附近或人潮聚集處。

(九)躲避安檢，司機獨自在車內。

五、如何遠離恐怖主義？

(一)拒絕接受恐怖組織吸收

恐怖組織的特徵：

1. 崇拜某位魅力領袖。

2. 中央集權組織。

3.主張採取暴力手段，對抗「邪惡」勢力。

4.團體生活、祕密結社。

5.對社會展現強烈排他性。

6.向成員施壓不得退出。

若參加之組織符合上述特徵，應保持冷靜，注意自身安危，逐漸疏遠，避免引起敵意，並立即報警。

(二)避免點閱恐怖組織相關網站

恐怖組織網站主要內容如下：

1.宣揚訴求

其訴求多屬偏激意識，表達恐怖分子的「委屈」，將恐怖攻擊活動合理化，以爭取同情與支持。

2.招收成員

偽裝成宗教或心理諮商，引導個人進入加密保護的網路聊天室，給予「心靈慰藉」。

3.籌募資金

以合法或非法手段，在網際網路籌募資金。例如：販賣物品（CD、DVD或書籍等)；利用慈善事業的名義，發送信件或張貼訊息，公佈捐款帳戶；偽造信用卡；引誘參加賭博。

4.散布謠言

利用謠言製造恐慌，煽動仇恨，或揚言發動恐怖攻擊。若發現上述內容，應避免再度點閱，並立即報警。

(三)救助可能受恐怖主義思想引誘的親朋好友

1.積極表達關心，瞭解對方獲得相關資訊的管道，受到引誘的原因，有無參與或資助相關組織或活動，是否接觸可疑人物等。

2.建議對方與其他親朋好友經常保持聯繫，並鼓勵參與正常社交活動。

3.對話時不可採取高壓逼迫方式，或直接予以指責，以免造成反效果。

4.立即向治安單位檢舉恐怖組織（分子)，並請求心理衛生、心理諮商機構給予協助。

六、接獲恐嚇威脅電話或郵件如何處理？

接獲來歷不明之電話或郵件威脅時，應立即報警，並依下列步驟處理：

(一)初步作為

1. 紙本郵件：將紙本郵件裝入較大的袋子。即使已拆封閱覽，請儘量不再碰觸郵件，便利警方採集指紋。
2. 電子郵件：將電子檔及列印之紙本交給警方，並保留原始電子檔。
3. 電話恐嚇：採取下列措施。
   (1)以「對話」代替「問答」，儘量獲取情報。
   (2)記錄時間、背景聲響、語言及口音。
   (3)保持鎮定，提示他人報警。
   (4)不可激怒或嘲弄來電者。
   (5)不可誇大其辭，製造恐慌。
   (6)若針對第三人威脅，請通知相關人員提高警覺。

(二)記下威脅內容

1. 對方之性別、年齡、種族、國籍、身分（恐怖分子、共犯、幫助犯、受害者或熱心民眾）及連絡方式。
2. 恐怖攻擊時間、地點。
3. 恐怖攻擊實施條件、動機、意圖及對象。
4. 犯罪工具（類型、外觀、數量）。
5. 恐怖分子位置。
6. 來電時間長度。

(三)所屬機關（單位）受威脅時，加強內部警衛措施。

(四)全力協助警方，切勿私下與恐怖分子交易、妥協。

七、報警時應注意什麼？

(一)保持鎮靜。

(二)確認目前是否危險。如有危險，迅速撤離或就地掩蔽。

(三)告知員警案發地點、時間、事件、結果、犯罪嫌疑人、犯案工具、逃逸方向、受害情形。

(四)現場如有人受傷，逕向消防機關或醫院請求醫療支援。

八、公共場所有哪些逃生設備？

處在陌生環境中，應避免進入通道狹窄，逃生出口不足之處所，並注意疏散通道方位及下列物品：

(一)警鈴、電話、對講機。

(二)室內消防栓。

(三)滅火器。

(四)緊急照明燈。

(五)鏈條梯或緩降機。

(六)逃生梯。

(七)緊急逃生路線圖。

九、如何撤離危險現場？撤離後之作為？

(一)保持鎮靜，辨別方位。

(二)建築物內發生爆炸時,恐怖分子很可能也在出口安裝爆裂物或伏擊，傷害緊急逃生人群，故逃生時要沉著判斷逃生路線。

(三)於火災或爆炸時不使用電梯逃生。使用樓梯時，隨手關防火門。

(四)只攜帶必要物品，不貪戀財物。

(五)不重返現場。

(六)保護身體重要脆弱部位。

(七)遠離玻璃，緊握固定物，靠邊行走。

(八)勿盲目跟隨群眾，守秩序地遵從指標（示)。

(九)如在行駛間之火車或高鐵列車內，勿強行開啟車門或跳下列車。

(十)快速行走、勿奔跑，幫助老弱婦孺。

(十一)擁擠時，一隻手緊握另一隻手手腕，雙肘撐開，平放於胸前，微微向前彎腰，形成呼吸空間。

(十二)不要逆著人流行動，以免被人群推倒踩踏。

(十三)被擠倒時，身體靠近牆角或其他支撐物，蜷縮成球狀，雙手緊扣置於頸後，保護身體的重要部位和器官。

(十四)保持救難通道暢通。

(十五)向親人報平安，並救助他人。

(十六)勿散播謠言。

(十七)勿進入受損之建築結構。

(十八)清查所有認識的人是否下落不明。

(十九)提供可疑人事物資料，如有影像等紀錄尤佳。

(二十)勿佔用緊急報案或醫療電話查詢一般事項，避免延誤救援。

防詐騙手冊-六種詐騙預防小叮嚀

★防騙第一部【假警察、檢察官辦案詐騙】

詐騙電話關鍵字：

銀行通知有人來領你的存款！ 警察通知你個人資料被冒用！檢察官說你是詐欺人頭戶！

★防騙第二部【購物個資外洩詐騙】

詐騙電話關鍵字：

向您核對購買商品日期、金額！ 說您收商品時簽單錯誤！

帳戶設定錯誤，變成分期付款！ 晚間 12 點後開始扣款！要去自動提款機取銷分期付款設定自動提款機沒有取銷分期付款功能

反詐騙小叮嚀：

預防上述詐騙，請牢記「一聽、二掛、三查」！

一聽！聽清楚這個電話說什麼？是否有以上關鍵字？

二掛！聽完後，立刻掛斷這通電話，不讓歹徒繼續操控你的情緒

三查！快撥 165 反詐騙專線查證！將剛才聽到的電話內容告訴 165

★防騙第三部【網路購物詐騙】

詐騙關鍵字：

開 msn，跳出交易平台，另談交易細節！ 商品已缺貨，要買要快！

賣家在偏遠地區不便當面交易，只受理匯款！不信可先付一半訂金，貨到再付另一半！

反詐騙小叮嚀：

1. 網路世界虛擬多變，請堅持面交商品。
2. 與市價相差太多商品，就要小心有詐。
3. 已買不到的商品如入場券，要考慮賣家的商品來源，為確保交易安全，務必堅持當面交易，並可請售票系統商家，查驗票卷真偽。

★防騙第四部【中獎、投資詐騙】

詐騙關鍵字：

【電話詐騙】公司舉辦抽獎活動，要您到場共襄盛舉！ 恭喜您已中獎！提供海外銀行電話可查證獎金已入帳！ 要交入會費、所得稅，才能領回獎金！

【網路詐騙】網友在海外是六合彩、賽馬會、投資顧問公司職員！提供投資機會！

電話通知您已獲利，快去匯款贖回獲利！ 海關查獲地下匯兌，要付關說費！

反詐騙小叮嚀：

1 中獎電話、公司地點、匯款銀行都在國外，查證不易，勿輕易匯款。

2.165 反詐騙專線數位資料庫，可協助查詢冒名詐騙公司名稱。

★防騙第五部【家戶拜訪詐騙】

詐騙關鍵字：

自稱是台電、瓦斯公司檢查管線！ 要更換水電、瓦斯管線並收費！

自稱是退輔會，關懷榮民訪問！ 自稱是社會局，老人居家訪視！ 可以申請生活津貼！

反詐騙小叮嚀：

預防家戶拜訪詐騙，請牢記「一關、二問、三查」！

一關！將大門關上，以防歹徒侵入家中。

二問！隔著門問來者姓名、單位、何事來訪。

三查！快撥 165 反詐騙專線查證！ 可查明來者身分以及到訪是否屬實。

★防騙第六部【假親友詐騙】

詐騙關鍵字：

自稱是您的親人（兒女、兄弟、姐妹）！自稱是同事、同學、軍中弟兄！先問候話家常！ 再藉口處理緊急狀況，或正在醫院向你借錢！

反詐騙小叮嚀：

1. 歹徒會以各種手段取得個人資料，再假冒親友熟人借錢。
2. 接到親友來電，並提出借錢要求，且不斷來電表示非常緊急，請以現在不方便接聽電話，先掛斷這通電話。
3. 找出自己的通訊錄，主動撥打親友電話號碼，並查證是否需要借錢。

資料來源：內政部警政署及 165 反詐騙網站~~