◎ 李忠憲

資訊安全威脅與防護

資訊安全不太像是傳統的自然科學，這門學問其實很複雜，
因為它要解決的不是自然界的問題，而是人製造出來的問題，
凡是人製造出來的問題都不容易解決。
它是一個除了技術以外，高度與人文相關的題目。

資訊安全不只影響到個人隱私，還是影響到國家安全層面的問題。

安全其實是個很弔詭的東西，理論上我們不怎麼重視安全。就像你今天不會因為安全的原因去買一棟房子，你買房子的理由一定是它地段很好、看起來豪華、裡面設備很棒、建材一流，房子買下享受到足夠東西，然後才會想到安全的問題。

但安全真的是很弔詭的概念。比如說買一輛車，車子裡配有安全氣囊。車子開個 25 年後都沒出什麼事，去報廢時裡面一打開，如果才發現是一顆石頭，並沒有安全氣囊，但我開了都沒事，也從沒爆開過，那我這個投資到底有沒有用？我為什麼要在上面投資？因此，資訊安全事實上不應該這麼紅，它是個配角，是個輔助，也就是當其他東西都有了以後，才會考慮安全的事。但安全不重要嗎？安全又重要的不得了。

當年美國 911 攻擊後過沒幾天，筆者前往美國開會，坐飛機到 LA 機場後要轉國內線，因為 911 發生在國內線，所以要轉去 San Antonio 之前在 LA 機場接受安檢就排隊排了 10 個小時。那就是為安全所付出的代價，但那時候有沒有人抱怨？沒有，大家都在那邊乖乖排隊。筆者就想說：「唉！怎麼讓我排這麼久？」因為大家很怕，很怕再出事情。因此，做資訊安全的人其實什麼都不用做，等到出事情的時候你就該上場了，只有出事情的時候才會感覺到你的存在。

因為這些背景因素，現在資訊安全已經牽扯到國安問題了。現在什麼東西都放上網路，包括軍隊、系統等資訊。因此資訊安全不只影響到個人隱私，而且已是影響到國家安全層面的問題。

資訊安全到底是什麼

以前在 PC 的時代，一人一台機器，很少能夠連上網。現在沒有什麼東西不連上網，甚至什麼東西都放到網路上面，這就是所謂的雲端。我們的資料基本上都放在雲端上，每個人都已脫離不了 Apple、google 等的世界，因此這個問題又變得更加複雜，尤其最近臉書的事件（個資外洩），大家又對資訊安全非常重視。在這樣的情況下，怎麼看待雲端網路資料安全這件事？

2018 年歐盟有一個資料保護法（General Data Protection Regulation, GDPR）開始要生效，雖然我們國家有個資法，但我們的個資法基本上作用不大，也沒有聽說有人因此受到罰款的報導。但歐盟這個 GDPR 保護法案可不一樣，它單一事件最高可罰一千萬歐元，或全球營業額的 2%。

有些台灣的大學還不知道這件事，如果你要做與歐洲相關的招生，學生裡面有從歐洲來的，都受這個法律的約束。這些都是在強調雲端上資料的安全，國網也在做一個類似國家的資料安全中心。這也是為什麼國家有個政策希望國網能建一個資料中心，而不是用國外的東西。我們當然不信任中國，那應該信任美國的一家公司嗎？

我們可以信任雲端服務的供應者嗎？安全一個很重要的基本概念是「信任」，那到底要信任誰？這就是一個很大的問題。尤其整個資訊系統在運作的時候，最簡單的是資料備份，或整個系統在提供服務上生產的備份，到底要信任誰？這都是一個沒有正確答案的選擇跟決定。

整個資訊安全的政策並不是下層的技術問題，上面的政策如果不清不楚，資訊安全的措施在公司或組織裡都是假的。

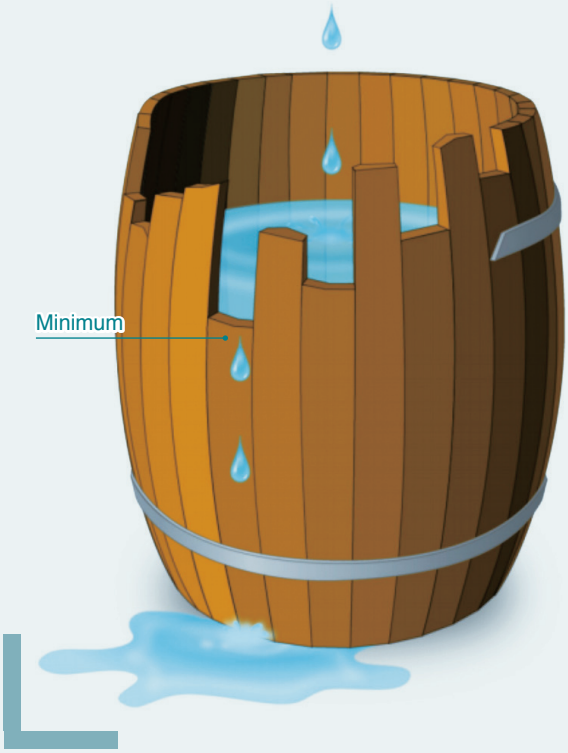
真實世界中的商務郵件詐欺

對個人來說，現在電腦有很多病毒、勒索軟體、分散式阻斷攻擊等。其實現在整個世界最嚴重的資訊安全問題並不是報章雜誌上常見的那些，而是 business email scam。什麼叫做 business email scam ？其實很簡單，本來 A 公司跟 B 公司的會計出納都有一個正常運行的模式，突然有一天，一個詐騙集團跟某一間公司說：「我是 A 公司，現在銀行帳號跟負責人已經改了，請你把原來匯款的管道改成匯到新的地方。」這是一個很傳統的詐騙方式，但現在是最嚴重的資訊安全問題，其中牽涉到的金額很可怕。

雖然這種詐騙手段很簡單，卻屢試不爽，被騙的金額很可觀，而被騙的公司都不敢講、悶不吭聲。這就是資訊安全中很弔詭的地方—我被騙了，可是不敢跟大家說。因為講了之後，你們不再信任我，我的商譽會受損，所以只好自己摸摸鼻子認了。

資訊安全基本上是什麼？筆者認為是領導力的問題。資訊安全是件很囉唆、麻煩的事，技術是最下層，技術上一層是管理，管理再上一層是政策，因此上面的政策如果不清不楚，領導力沒有展現出來，資訊安全的措施在你的公司或組織裡都是假的。講很容易，但做很困難。

以前筆者在成大計網中心服務的時候，光學校 email 的帳號每 3 個月到 6 個月改一次密碼（原先有的資訊安全政策），就很難做到了。那陣子硬要推這個政策，常常有教授打電話來罵，甚至有一位醫生打電話罵：「你叫我換密碼，我已經忘了哪一個是正確的密碼，你來幫我看病，我的病歷系統打不開！」那時候你要怎麼辦？筆者當時只是計網中心網路組的組長，可是這是領導力的問題，要校長、副校長那樣層級的人才能回答。因此整個資訊安全的政策並不是下層的技術問題。



短桶理論，能決定盛水量的是最短的那一塊木板，而不是最長的。

資訊安全的概念—短桶理論

資訊安全的概念最基本的是「木桶原理」或「短桶理論」，也就是在木桶子裡能夠盛多少水，不是取決於最長的那一塊，而是最短的那一塊，因此系統最弱的地方就是整個系統能力的所在點。這個大家都很清楚，比如說在家裡有前後兩個門，還有左右兩邊窗戶，前門用十道鎖防護好，後門卻開著，你的家就一點安全也沒有。

資訊安全也是這樣，如果有人跟你說這個系統的資訊安全絕對沒問題，這句話本身就有問題。資訊安全有句話說「絕對的資訊安全表示絕對的破產」，也就是你

防火牆好比是堅固的城門，阻絕外部的資料進入受保護的機器內。（圖片來源：種子發）

花再多的錢去弄很長的那一塊，錢再怎麼花都不夠用，你一定有很短的那一塊，因此在資訊安全的術語裡很強調一個概念就是一致性。什麼是一致性？就是整個系統所有環境大家防護的資訊安全能力要差不多，你不用花大錢，可是要差不多，有什麼能力就做什麼事，而且要差不多。

因此又牽扯回來，資訊安全不僅是技術的問題，因為往往出問題的地方在人，人一定有疏忽的時候，一定有弱點，這也是資訊安全裡最麻煩的事情。如果用一個簡單的概念來講，資訊安全有如中古世紀的城堡，城堡裡面有士兵，外面有高聳的城牆，這高聳的城牆就是各種防毒軟體，另外有防火牆，它是堅固的城門。另外有一些網路保護的機制，比如入侵偵測系統、分散式阻斷攻擊的清洗設備等，這大概是一般資訊安全的情況。

目前的防毒軟體可抓到的病毒很少，因為病毒變種又快又新，等到這些東西都知道了，有它的 signature 的時候，都已經過一段時間。因此真的能抓到病毒的防毒軟體比率其實不高，防火牆跟一些網路保護的機制大概還可以發揮一些功能。

對一個組織來說，安全資訊的分享非常重要，且這個組織要常常舉辦資訊安全的講習。這個講習的主要目的第一個是修補資訊系統的漏洞，也就是亡羊補牢，把一些知道問題的地方藉由更新來修補，才能降低被入侵的風險。第二個是提高警覺，要修補使用者的習慣，透過教育養成資安的意識。現代人的生活不可能離開資訊系統，已經不可能沒有手機、沒有信用卡，或不用行動支付、不線上購物、不線上買票。但在這種情況下，一定要有資訊安全的意識，才能保護自己及朋友，因此說「資訊安全，人人有責」。

在這人手一機的時代，個資保護格外重要。（圖片來源：種子發）

資訊安全三要素

資訊安全最基本有三個要素，稱為CIA。

機密性（confidentiality）—採用適當的安全機制保護資料和資源，以避免暴露在無權限人員或程式之下，而危害到資訊安全。

完整性（integrity）— integrity 在英文的字義是這個人做人很一貫，可以信任他。但在資訊安全上指的是完整性，確保維持資料原來的狀態。有時資料的機密性沒這麼重要，反而完整性比較重要。譬如說股市開市時說要下單買 100 張台積電股票，結果台積電那天跌停板，就說：「沒有，沒有，我沒有要買！」這就不行，沒有完整性。資訊有時有沒有機密不重要，但如果內容被竄改，就失去資訊的完整性，就違反了資訊安全。

可用性（availability）—確保資訊與系統能夠持續經營、正常運作。一般大家重視的就是這個可用性，比如說電話要能夠通、網路要能夠通、訂票系統要能夠運作等，沒有這些的話會造成問題，因此可用性是資訊安全三要素中的一環。

當然還有其他的如：不可否認性、驗證性、授權、可究責性。可究責性是數位鑑識的主要基礎，現在有關數位鑑識的領域很紅，資訊安全在全世界都缺人，一些年輕朋友如果找不到人生的方向，資訊安全保證是個很有前途的行業，而且它所需要的知識領域與人才是各種類型的。大家不要想說需要的資安人才就是駭客，

資訊安全的三要素（機密性、完整性與可用性）常常會互相影響，而且彼此之間要有所取捨。

這根本是錯誤的觀念，我們要的資安人才是資安專家。什麼是資安專家？駭客是找到一個系統的漏洞就攻下去；而資安專家是要把所有系統的漏洞照顧好。

資訊安全的三要素（機密性、完整性與可用性）常常互相影響，而且彼此之間要有所取捨。比如說，這個加密系統非常棒，這個 key 在你有生之年都破解不了，可是用了這個協定後，系統慢得不得了，「我很安全，但我很慢。」這該怎麼辦？這樣就變廢物了，「我很安全，但我是安全的廢物。」反之，這系統很快，可是三兩下就被別人破解，這樣也不行，用這個系統比不用還危險。因此這三者之間要妥協，或是選擇價值的問題。因此資訊安全或相關的學問，有時候很不像自然科學，比較像人文科學。

另外，一個組織需要一個資訊安全政策。在一般公司中，資訊安全越來越重要，因此要做一些資訊安全政策的管理目標，同時要做一些風險的管理。像是公司裡面有什麼東西是核心資產，這些東西不能動，不然公司會倒。這樣風險有多大？要用什麼措施來降低風險？這些相關的內容基本上是資訊安全政策所需要的部分。

資訊安全這東西是突然在網路的時代冒出來的。在 1970 年代，離現在還沒有很遠的時候開始有網際網路。網際網路在一開始設計的時候僅限於學術界及一些相關單位，當時是美國的學術單位發現有一堆電腦，這些電腦本來有一些簡單的連接方式，如 Unix 系統或 Unix pipe 把這些連結在一起，這些科學家就思考如何連得更多。

一開始是把 3、4 個節點連起來，想不到沒隔多少年網際網路的發展如此快速，把很多日常生活上的行為直接搬上去。而它原先的設計、邏輯和使用者跟現在相差非常大，以前就是學術和研究單位用的，這裡面的人雖然不是沒有壞人，但組成分子基本上比較單純，並不像一般社會這麼複雜。這實在是當初設定網路協定的人完全沒有預想到的，他們沒有想到這個問題，因此才有資訊安全的發展。

筆者在成功大學教書快 20 年，從教書第一年就教通訊網路的課程。那時通訊網路課程的教科書完全沒有網路安全這一章，沒有人想到會有這個問題。而最近 10 年內這樣的問題才慢慢浮現出來，有高瞻遠矚知道這問題的人並不多，但這個問題的嚴重性的確很大。筆者本身博士是在德國念的，德國這國家令人佩服的一點是他們對很多事情很有遠見，德國在 1990 年在內政部就成立了聯邦資訊安全局。1990 年！1990 年我們在幹什麼？我們 1990 年怎麼知道會有這個問題？

當時面臨到的現實是「網路這麼慢」、「東西不太會動」、「電腦三不五時就當機」，怎麼知道這是一個重要的事情，但德國做到了。資訊安全當然大家是搞不清楚的，筆者原來也不是做資訊安全的，念書時也沒有資訊安全這門學問。剛回成功大學時，說在做資訊安全的都是在做數學，那些很難的加解密數學是他們主要的研究，跟日常生活和網路協定及資訊系統有一段距離。

就好像天才兒童楊柏因在做的後量子時代的密碼學，科技部說每年要花 7 千萬在量子電腦上，原來加解密的方法在量子電腦時代都不能運用，很容易被破解。

網路的時代就是這樣，因為大家都在用，尤其臉書又不用花錢，以前怎麼會想到這種 business model，十幾億人在用都不用花錢，而且很好用，系統又穩定又快速。但是大家用這種不用錢的東西，難道不會心裡毛毛的？

國內外資訊安全事件與趨勢

香港公投網站遭 DDoS 攻擊事件 2014 年 PopVote 線上投票網站就遭遇到超大規模的 DDoS 攻擊，攻擊流量達網路史上第二高，連找 Amazon 或 Google 網路服務支援都擋不住。CloudFlare 最後靠著全球網路服務業者聯手，才撐過這 10 天的投票過程。

根據 Google 從 6 月 14 日當日偵測到的全球網路總攻擊頻寬顯示，其中鎖定香港 PopVote 網站的網路攻擊活動遍及世界各地，以各種 DDoS 攻擊手法，如 DNS、NTP 進行大規模網路流量的癱瘓攻擊。

DDoS（Distributed Denial-of-Service）指的是分散式阻斷攻擊服務，基本上網路協定先天的設計就是假設大家都是好人，在大家都是好人的情況下，你要求我提供服務給你，通常是沒有問題的。因此在協定上面的設計，你給我個要求，我就要做一些回應。

可是當要求越來越多，或用其他形式的要求呢？例如像雪崩式的要求，整個系統就會癱瘓，這稱為 denial of service。Denial 就是否定的意思，也就是這個服務基本上就沒有了。那什麼叫 distributed 呢？distributed 是指分散，分散的意思是一個人攻擊你沒什麼力量，你可以很快抓到，可是如果是一次從各地幾千、幾百萬人攻擊你，你要防護就比較困難。

其實 DDoS 攻擊有點像是軍備競賽，就是今天你攻擊我，而我有多少能力來抵抗你的攻擊。像大家常覺得 google 很穩，連 DDoS 也攻擊不了。據聽到的消息，google 可能有幾萬個或幾十萬個 server 用高速網路串接在一起，因此你要打它沒那麼容易。

但你要打掛其他企業的網站，其實並不是件很困難的事，可是要打掛像 google 這種大的網路服務公司的 service 是很難的，並不是說它的技術或能力有多好，而是它有那樣的 capacity。在這個軍備競賽中，它守的部分是可以比得過攻的。現在 DDoS 攻擊的手法有很多種，細節就不在這裡提，但這類攻擊的事情是越來越嚴重，而且流量一直不斷在擴增（指單一事件）。

南韓水力與核電公社（KHNP）傳出遭駭客入侵 2014 年 12 月自稱為「反核子反應爐集團主席」的駭客公布南韓核電廠的平面圖、操作手冊，與超過 1 萬名 KHNP 的員工資料。要求南韓限時關閉 3 座核子反應爐，否則就要釋出更多機密資訊。

KHNP 自行調查，結果發現共有 12 種類型，117 件資料外洩。根據外電報導，南韓政府調查發現駭客利用了美國、日本與南韓的虛擬私人網路等不同路徑以迴避追蹤，最原始的攻擊 IP 則來自中國的瀋陽。

駭客攻擊已經入侵到水跟核電。2014 年 12 月，核電廠的平面圖、操作手冊及超過 1 萬名的員工資料全部被公布。在以前，網路攻擊只是騙騙錢、偷偷資料，威脅一下叫你匯比特幣。現在已經不是這樣了，已經入侵核電廠、水庫、高鐵等，這些事件最後會變成恐怖攻擊，造成重大的人員傷亡。這時資訊安全已不是詐騙或錢的問題，而是牽涉到人命的問題，這也是為什麼資訊安全越來越受到重視。

現在筆者有一部分計畫在執行有關電廠或一些關鍵基礎設施的工業控制系統，這些工業控制系統都很舊，而且這些系統通常沒有人願意去碰它，可能 30、40 年都沒人動，或沒人敢動，基本上這些系統的弱點跟漏洞很多。

關鍵基礎設施有可能受到駭客攻擊的威脅，這時資訊安全已不是詐騙或錢的問題，而是牽扯到人命的問題。

但問題是，因為物聯網、感應器等越來越普遍、便宜，很多系統都慢慢布建進去，因此工業控制系統與資訊系統是有一定程度的掛鉤連結。然後這些資訊安全的危險，就會從資訊系統這邊外溢到工業控制系統那一邊，這是一個新的挑戰，也是我們國家資安管理法有規範到關鍵基礎設施的原因之一。

最後做個結論：

（1）資訊安全是個需要技術輔助的「管理」議題。它不只是技術，很多是leadership的問題，對於所有人員、流程和技術要有一個規範。資訊安全包含的內容和學問很多，不單只是一個技術的問題。

（2）以金融機構為目標的攻擊案例日益增多，且攻擊者仍使用存在已久的社交工程攻擊手法，還是能有效入侵大公司，造成其金錢上的損失。機構或公司應持續著重提升人員的資安意識，以降低社交工程手法成功的機率。

（3）更多案例顯示委外廠商本身也已成為駭客竊取資料的對象，有鑒於委外供應商資安風險持續提升，應建立委外廠商資安要求標準，律定其資安監控與事件通報的責任與義務。

自 2013 年觀察到駭客已開始利用軟體供應商做為跳板的趨勢，這個世界已經不知該相信誰了。有很多人說不應該用電腦、資訊系統，但這些東西你逃不掉，除非到深山隱居，而且可以不傳美麗風景的照片跟你的朋友炫耀。不然還是得用，但要用就要重視資訊安全跟隱私。

李忠憲
成功大學電機工程學系 / 國網中心