壹、資安新訊

交通領域關鍵基礎設施提供者注意

《交通部交通領域工業控制系統資安防護基準》(下稱交通領域工控防護基準)已於今(2022)年核定，此基準將資通安全責任等級分級辦法(下稱分級辦法)附表十防護基準之規定，配合工業控制系統(ICS)之特性，重新編排並進行調整。除納入並調整防護基準已有之存取控制、事件日誌與可歸責性、營運持續計畫、識別與鑑別、系統與服務獲得、系統與通訊保護、系統與資訊完整性等構面之內容外；交通領域工控防護基準並增列部分細緻之實體安全規範，例如設備機房之安全作業、設備安全管理，以及明述ICS網路之網路安全規範、人員管理規範等。

資通安全管理法納管之對象，原則均應依其資通安全責任等級，辦理分級辦法附表所定應辦事項，若有自行或委外開發之資通系統者，並應完成該資通系統之防護需求等級評估，辦理對應之系統防護基準控制措施。其

貳、國際觀測

德國2021至2025年國家網路安全戰略重視事件應變

為強化聯邦政府之資安防護，德國自2011年起，提出5年期的國家網路安全戰略。繼2016年第二期後，2021年9月發布最新之第三期戰略(2021至2025年)。該戰略透過指導方針、行動領域及戰略目標之組合，描繪德國在網路安全相關領域之應有基礎與長期發展方向。

目前規劃4項行動領域，搭配各領域之戰略目標，予以落實：

1.數位化環境中之安全與獨立行動。

2.國家與經濟的共同任務。

3.高效與可持續之全國網路安全架構。

4.歐洲與國際網路安全政策中之積極定位。

以領域3為例，考量前二期較未落實處，並配合2021年5月資安法2.0施行，該戰略迄自2022年8月，近一年來持續透過增加預算、人力等方式，促進聯邦政府、各邦間密切合作，除確保網路空間之安全，也有助於改善

中之防護基準控制措施，依分級辦法第11條第2項規定，得由中央目的事業主管機關就特定類型之資通系統另定之，並經主管機關核定後辦理。交通領域工控防護基準，即交通部針對所管特定非公務機關之自行或委外開發「交通領域工業控制系統」所定，並函知其所管特定非公務機關，以利其等參考辦理。
資料來源：行政院111年4月20日院臺護字第1110011191號函

聯邦政府因應網路攻擊之能力，有利於事件應變。
資料來源：BMI, Cybersicherheitsstrategie für Deutschland, https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/cyber-sicherheitsstrategie/cyber-sicherheitsstrategie-node.html

參、重要案例

上市公司遭勒索軟體LockBit 2.0攻擊，外洩資料141GB

【焦點話題】

國內某上市營建公司發布重大訊息，表示內部部分資訊系統遭受駭客網路攻擊，資安團隊於第一時間啟動防禦機制及備援作業，並通報執法部門。四日後，該公司之關係企業即某興櫃公司亦發布重大訊息，表示部分資訊系統遭受駭客網路攻擊，發言人聲稱係因二公司之資訊系統共用，屬於同一事件。
暗網LockBit 2.0資料外洩的公布網站，傳有上開上市營建公司的被駭頁面，應可確認LockBit 2.0勒索軟體是該公司資安事件的肇因，據稱外洩141GB的資料，駭客並向公司勒贖8萬美元。

【重點摘要】

1. 勒索軟體（ransomware）是一種利用加密技術的惡意軟體，而LockBit為一種著名的勒索軟體。加密（encryption）係以加密演算法與金鑰使資料由明文（plaintext）轉換為不可理解之密文（ciphertext），以保護資訊之機密性。勒索軟體則反其道而行，以未經授權之加密，造成使用者無法存取資料，駭客再藉機向企業或使用者勒索。
2. 駭客入侵公司資訊設備、竊取其中資料，再以勒索軟體加密公司檔案，使公司無法存取被加密的檔案，並導致系統無法運作，喪失或減損其可用性，將可能觸犯刑法第358條之無故入侵電腦罪、第359條之無故取得他人電磁紀錄罪，以及第360條之干擾他人電腦罪。
3. 面對各種資安威脅，現代企業的資安思維應由「如何防止各種資安事件」進一步到「在資安事件發生時，如何使企業在最短時間內恢復運作」，系統備援及資料備份是最核心的關鍵。公司由於對於系統及資料均有合理的備援、備份，因此在遇到勒索軟體攻擊時，得以迅速回存系統與資料，恢復運作。

【法律分析】

資料儲存容量、處理速度與傳輸頻寬隨著科技發展而急速升高，資料的產量空前驚人，而企業內部的資料質量俱高，往往為駭客所覬覦。駭客先綜合弱點掃描、社交工程、釣魚、水坑式攻擊等手法，探知組織的系統或應用程式漏洞、成員的帳號、密碼等驗證資訊，進而找到入侵的機會，入侵後先不動聲色，在組織內部持續埋伏、擴張，尋找有價值的標的，待尋得後低調傳輸至外部，甚至將組織內部之系統或機密、重要檔案加密，使組織成員無法存取檔案，或使系統根本無法運作。現代企業規模龐大，客戶及股東眾多，一旦受損，往往株連甚廣，面對駭客集團化且無時無刻的威脅，更應妥善應對。以下從駭客攻擊及企業因應兩個面向，簡析相關法規：

一、駭客攻擊相關法規

《刑法》妨害電腦使用罪章，大致對於以上的駭客攻擊行為加以規範：

1.駭客突破電腦的保護措施而入侵，此時雖然尚未造成被入侵者的實質損害，但是入侵者可能可以對於電腦內的系統或檔案予取予求，對於以下提到的資安三角（CIA Triad）—機密性、完整性與可用性直接形成威脅，風險有秘密性，也就是其價值常取決於其是否能保持不被民眾或競爭對手知悉，此即「機密性」（Confidentiality）。就此而言，駭客猶如「資訊竊賊」，竊取有價值之資訊後，可在黑市（暗網）標售，價高者得，亦可回頭威脅企業，若不給付金額，即公諸於世。本案駭客共取得141GB的資訊，破壞了資訊的機密性，構成《刑法》第359條無故取得電磁紀錄罪；

3.本案駭客在竊得企業資訊後，以勒索軟體將儲存在企業的檔案加密，使得企業對於這些檔案「可望而不可即」，檔案加密後，仍然存在於電腦中，但卻無法開啟，除非駭客提供金鑰，否則無從知悉內容與運用。對於企業而言，對於這些資訊的可用性已遭破壞；從被加密的資訊本身而言，也可謂資訊因變更而失其完整性（Integrity），構成《刑法》第359條無故變更電磁紀錄罪。

4.本案駭客以勒索軟體加密的對象還包括了系統檔案，使電腦等設備難以運作，破壞了資訊系統的可用性（Availability），可謂對於電腦的嚴重干擾（interruption），構成《刑法》第360條無故干擾電腦罪。

的，是對於此類資安事件發生後，得以迅速恢復運作，也就是營運持續計畫的規劃與執行。《資通安全管理法》第7條第1項授權主管機關行政院制定《資通安全責任等級分級辦法》，其中附表十《資通系統防護基準》就營運持續計畫訂有系統防護與控制措施，即使企業尚非資通安全管理法之適用對象，仍值得參考，略述如下：

1. 系統備份：亦即將系統恢復所需資料進行備份，需求分級與控制措施如下：

(1) 普級：分成二部分，其一為訂定系統可容忍資料損失之時間要求，此又稱為「復原點目標」（RPO）；其二則為執行系統源碼與資料備份。

(2) 中級：除普級的所有控制措施外，尚應定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。

(3) 高級：除中級的所有控制措施外，尚應：

① 將備份還原，作為營運持續計畫測試之一部分；② 應在與運作系統不同處之獨立設施或防火櫃中，儲存重要資通系統軟體與其他安全相關資訊之備份。

2. 系統備援：中、高級之控制措施如下：

(1) 訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。此即「復原時間目標」（RTO）

大幅提高，而可能構成《刑法》第358條入侵電腦或相關設備罪；

2.早期的駭客入侵，常為了樂趣與炫耀能力，現代的駭客入侵，則通常為了利益。企業所擁有的資訊通常具有較高價值，而且多具

二、企業因應

承上，勒索軟體對於企業的系統與檔案加密，使得企業對於資訊之可用性受到破壞，嚴重影響企業的運營、信譽及財產權益。因應之道，除了對於可能的入侵管道盡力防禦之外，最基本而重要

(2) 原服務中斷時，於可容忍時間內，由備援設備取代提供服務。

【管理要點】

一、 入侵之防範

本件駭客係先行入侵公司資訊設備，再竊取資料，並以勒索軟體加密公司檔案。至於駭客入侵之手法，並未公布，不外乎係利用企業員工之資安意識薄弱，以社交工程（social engineering）騙取登入資訊、誘使下載惡意軟體，或是攻擊未及修補之系統或應用程式漏洞。防範之道，為以下兩點：

（一）提升員工資安意識

就資訊安全防護而言，最脆弱的一環往往在於「人」，尤其是一般使用者，使用資訊設備時常貪圖方便，疏於注意資訊安全，以致使駭客有機可乘，一旦有使用者被突破，資安防護即出現缺口，而可能潰堤，造成企業重大損害。

因此，對於員工定期施以教育訓練，並且不定期舉行社交工程演練，逐步培養員工的資安意識，才能盡量降低「人」的風險。

（二）即時更新與弱點掃描

現代資訊系統與應用程式動輒以數百萬乃至數千萬行程式碼所構成，內容與功能極其複雜，因此並不存在無漏洞之系統與程式，各廠商也不斷就新發現的漏洞予以修補。而自發現漏洞至修補漏洞，不免出現一定之時間差，遂有「零時差漏洞」（zero-day vulnerability）的出現，駭客搶在修補程式出現前，針對漏洞設計出攻擊程式與手法的情形屢見不鮮。企業應盡量即時更新系統與程式，並定期執行弱點掃描。

二、 持續營運管理

資安防護，向來即無盡善盡美之可能，應同時考量設施的重要性、風險評估，以及個別設施特重機密性、完整性或可用性，在預算之內達成妥適管理。本案駭客的手法，係同時攻擊資訊之可用性與機密性，而受害企業分別為上市及興櫃公司，資本雄厚，股東眾多，影響層面廣泛，企業之持續營運應優先考量。機關之持續營運管理，包括事前的風險評估（Risk Assessment）以及營運衝擊分析（Business Impact Analysis），以及資料、系統之備份，以及機房等設備之備援，均屬基礎而重要。

肆、經典文摘

在競爭中尋求合作：美國金融服務業的資安夥伴關係

[編輯推薦]
在關鍵基礎設施(CI)的資安防護上，若主管機關與私部門的CI提供者間，能保持良好而密切的合作關係，無疑將會使資安的防護更完善，但如何合作才能達到最好的平衡，則始終是一項需要討論的議題。
本期編輯所摘要介紹之經典文獻「在競爭中尋求合作：美國金融服務業的資安夥伴關係」(以下簡稱「資安夥伴關係」)，即以公私合作為題，該文作者選擇美國金融服務業作為觀察對象，分析其公私合作成功的因素，以及密切的合作關係所帶來的優缺點，頗具參考價值。

一、文獻資訊

[原文標題]
Cooperation amidst competition: cybersecurity partnership in the US financial services sector
[作者]
Sean Atkins, *Department of Political Science, Massachusetts Institute of Technology, Cambridge, MA 02139, USA*
Chappell Lawson, *Department of Political Science, Massachusetts Institute of Technology, Cambridge, MA 02139, USA*
[出處]
Journal of Cybersecurity, Volume 7, Issue 1, 2021, tyab024, https://doi.org/10.1093/cybsec/tyab024

二、重點內容

現今關鍵基礎設施的資安受到高度威脅，而其中一種有效的防護方式即為公私部門間強化資安合作關係。「資安夥伴關係」一文的作者即指出了美國的金融服務業為資安公私合作的一個重要成功範例。該文作者的研究方式除透過公開可取得的資料進行外，並訪談了在公私部門合作中不可或缺的重要角色：資安從業人員，以了解相關合作模式是如何(how)、又為何(why)形成的，以分析合作成功的關鍵。
以歷史背景的脈絡而言，美國金融服務業發展是許多因素交互作用的結果，包括時間、行業的風險程度，以及公司的特徵(如規模、市場定位)。對一個金融業者而言，有許多單位在監管它：聯邦機關、州機關，以及一些金融業的組織，各自針對不同的重點，例如存款、信貸、支付系統等，進行管制或規範，因此法遵要求也隨之複雜。為了因應這樣的複雜性，在資安議題上，金融業組成了情資分享平台FS-ISAC(Financial Services Information Sharing and Analysis Center)，讓業者可以和政府定期開會討論產業的資安問題，簡化負擔；而在FS-ISAC架構下，幾家主要的大銀行又成立了FSARC(Financial Systemic Analysis and Resilience Center，金融系統分析與彈性中心)，再進一步強化了公私部門間面對資安威脅時的緊密聯繫。
另一個能夠強化上述公私部門間在FS-ISAC合作的因素，則源自一個美國金融服務業的特殊現象：許多大公司的資安專業人員都是自公部門，例如軍隊、執法機關等招攬而來。
作者總結美國金融業FS-ISAC制度成功關鍵包含數點：
1.由於公私部門都充分了解資安威脅的嚴重性，促使企業高層願意積極和政府合作。
2.在行政監管層面，為了避免輕忽資安所可能導致的法律責任，企業願意導入相關的資安標準。
3.在金融產業中，公私部門之間有長期建立的良好互動關係。
但另一方面，也有一些因素不利於協力：
1.規模較小的企業可能較不願意投資資安防護。
2.雖然接收分享而來的情資有助於企業加強資安，但當企業自身發生資安事件時，則可能因為擔心商譽受損不願進行通報。
3.金融業受到高度監管的特性也讓企業對於要和政府機關分享資訊採較保守的態度，分享的資訊愈多亦意味著被政府掌握的愈多。

金融服務業的組成類型十分多元，常見的如銀行、證券、保險、經紀或租賃均屬之，但金融業者的類型會影響到其關注的資安重點，例如保險公司主要注重個資保護，經紀業者則最擔心勒索加密。與此同時，產業整體所面臨的資安威脅來源也十分多樣，從個人、組織型駭客到國家都有，不易抵禦。

4.當企業面臨來自多個不同的監管機關的要求時，這些監管機關在資安上的要求也可能不一致。