國際貨運代理協會聯合會（FIATA）提議的最佳做法

防範網路犯罪

fiata.com

免責聲明

請謹記，本檔不包含任何法律意見。如果讀者對資料保護法律或其他法律相關問題存有任何疑問，我們建議讀者諮詢法律專業人士。

另謹請注意，這些最佳做法主要是從風險管理角度給予的一般性指引，而非技術建議。公司應根據自身具體公司結構、商業模式和風險管理要求調整及實施建議措施，並徵詢國家主管部門、FIATA 協會會員或技術專家的技術協助意見。

FIATA 對使用本文件所含資訊可能所引發的後果不承擔任何責任。

如需更多關於 FIATA 法律事務諮詢委員會活動的資訊或對本指引有任何意見，請聯繫 FIATA 秘書處 info@fiata.com

DISCLAIMER: The Best Practices Guide on the Prevention of Cybercrime was translated into Chinese by TT Club's office in China and proofread by the chair of the FIATA Asia-Pacific region. In case of a discrepancy, the English original version will prevail.

FIATA 提議的最佳做法

防範網路犯罪

為協助 FIATA 協會會員和個人會員以及全球物流和貨運代理行業，FIATA 法律事務諮詢委員會（ABLM）特編制本最佳做法指引。

對於貨運代理領域從業者而言，無論是在自身所屬司法轄區還是在國際範圍內經營業務，法律問題都是很關鍵的。因此，不斷告知貨運代理人世界各地的法律發展情況，與建議協會根據法律發展採取保護其會員利益的行動一樣，是 ABLM 最為重要的工作。

ABLM 擁有 12 名委員和眾多來自世界各地的增補委員，他們都是經驗豐富的法律從業者、教授或活躍的貨運代理人。ABLM 每年會在蘇黎世總部和 FIATA 世界年會舉行兩次會議，兩次會議都是歡迎全球貨運代理人的參與的公開會議。

在過去的幾次 ABLM 會議上，ABLM 的法律事務專家曾向 FIATA 會員報告行業內網路犯罪數量增加的情況，與會者對這一主題表現出了極大的興趣，並請求 ABLM 給予如何降低網路攻擊風險方面的建議。

隨著資訊技術日益廣泛的應用，國際運輸和物流行業面臨的網路犯罪風險正在不斷增大。如今，隨著物流服務提供者正逐漸成為資料驅動型的組織，客戶、價格和運輸方面的資料的數位存儲率正日益增長，但與此同時，這也增加了數字基礎設施被攻擊的可能性。

過去的幾年，見證了一系列行業龍頭企業受到網路攻擊並因此遭受供應鏈嚴重遲延和經濟損失的事件的報告。需要注意的是，這些企業大多數並非攻擊的直接目標，而是隨機受害者。在網路攻擊突破了企業防禦的情況下，企業需要花費大量的時間和金錢，來阻止攻擊、通知客戶、重新安排供應鏈以及彌補其他後果。

現在許多司法轄區的法律，都明文規定企業應當保護機密資料和/或個人資料。例如，歐盟的《一般資料保護條例（GDPR）》要求歐盟公民個人資料的持有者在處理和傳送資料時須採取某些特定措施，並在資料遭受嚴重破壞時通知客戶和主管當局。國際物流供應商和貨運代理人很可能屬於這項法律的適用範圍，因為他們持有客戶和貨運的資料。

鑒於 FIATA 會員的請求、網路犯罪帶來的威脅以及新的政府政策和法律的要求，ABLM 製備了這份檔，旨在提高 FIATA 會員和行業從業者對網路犯罪威脅和風險的認識、介紹評估及減少風險敞口的推薦措施、以及就防範網路犯罪的最佳做法提出建議。

FIATA 特別鳴謝聯運保賠協會（TT Club）的邁克爾．亞伍德（Michael Yarwood）先生，其對本文做出了重要的貢獻。

摘要

網路犯罪系因資訊技術系統故障而導致的風險，形式多種多樣，如網路釣魚、魚叉式網路釣魚、惡意軟體、付款授權欺詐或勒索軟體。

在過去 5 年中報導了許多與網路有關的事件，其中一小部分受到高度矚目的案件，牽涉物流及貨運代理行業。

由於現在的業務都嚴重依賴資訊技術系統，資訊技術系統一旦中斷或暫停運行、或者客戶和運輸資料庫一旦遭到破壞，運輸業務的經營以及與客戶、承運人和分包商的溝通都會受到嚴重干擾，進而造成金錢損失和潛在法律責任。

ABLM 建議物流服務供應商和貨運代理：

- **評估風險敞口：**識別在資訊技術（IT）系統中和操作技術（OT）系統中可能受到網路攻擊和出現運行漏洞的區域
- **採用技術標準**，例如 ISO/IEC 27000 系列標準或關於物流行業資訊安全的國家標準
- **採用一般防範措施**：在無法實施具體技術標準的情況下，採用如下措施：
  - ✓ 實施多級防禦，如硬體物理安全、管理程式、防火牆和系統架構、電腦策略、帳戶管理、安全升級和殺毒方案。
  - ✓ 按照“有必要知曉”原則限制公司內部資訊存取權限
  - ✓ 採用隔離和協定感知過濾技術保護關鍵系統
  - ✓ 採用網路加固措施，確保補丁管理充分並且受到積極審查
  - ✓ 對 USB 等設備的接入和使用，採用可移動設備策略
  - ✓ 對協力廠商供應商進行審查，以確保網路安全符合要求
- **制定業務連續性計畫**，以應對需要對攻擊做出回應的情況
- **實施儘快探測到網路攻擊的措施**
- **成立由核心人員負責的緊急應變小組**
- **堅持組織員工培訓：**經常組織安全意識簡介會及培訓專案，對所有員工進行最佳做法教育，以確保全體員工知曉、瞭解並遵守法規要求
- **確保公司投保適當的保險**，為業務提供一定程度的保護

什麼是網路犯罪？

英國風險管理學會將**網路犯罪**定義為“任何組織因其資訊技術系統的某種故障而遭受經濟損失、干擾、聲譽受損的風險”。

與網路犯罪有關的風險敞口的範圍非常廣泛，包括滲入到組織資訊技術系統中的人員、組織的程式/人員的弱點。網路攻擊的形式多樣，常見的例子為網路釣魚、魚叉式網路釣魚、惡意軟體、付款授權欺詐或勒索軟體。

網路攻擊對於一個組織而言可能是極其有害的，通過阻斷服務這一攻擊手段，不僅會造成巨大的經濟損失，還會造成不可挽回的聲譽損害。網路攻擊還會妨礙企業有效運營，使其無法滿足客戶需求。

真實的威脅

在過去 5 年中報導了許多與網路有關的事件，其中一小部分受到高度矚目的案件，牽涉物流及貨運代理行業。

網路事件五花八門，種類從簡單的付款授權欺詐騙局，到勒索軟體攻擊，再到針對特定資訊技術基礎架構的攻擊，花樣頻出。對於這樣的風險敞口，並沒有一刀切的解決方案。需要強調指出的是，迄今為止大多數案件均非針對性攻擊。

現如今，進行這種攻擊的手段也正變得更加廉價，也更加容易獲得。網路犯罪分子可以從暗網購買網路犯罪服務產品，在犯罪分子技術能力有限的情況下，這些產品起到了促成網路犯罪的作用。

2017 年 6 月，A.P.穆勒-馬士基集團（A.P. Moller Maersk）成為一場名為“非佩提亞”（Notpetya）的全球無針對性惡意軟體攻擊的受害者。馬士基的商業活動受到了廣泛影響，包括網上訂艙、一般性電子郵件通信、與客戶溝通的能力以及全球多達 76 個港口碼頭的運營管理均受到了影響。雖然馬士基能夠迅速從攻擊中恢復過來，但據報導該攻擊還是造成了數億美元的財務影響。

21 世紀的企業嚴重依賴於自身資訊技術基礎架構。許多員工從不知道以前的手工操作方式，因而完全依賴於資訊技術基礎架構帶來的自動化和高效率化。物流和貨運代理行業服務於全球的特性及對資訊技術系統的依賴，使得該行業成為了易受攻擊的潛在目標。

犯罪者：動機和目標

實施網路犯罪的犯罪者有很多，各個都有自己的動機和目標。將他們分組並概括他們的動機，對於更好地瞭解網路攻擊對貴司構成的威脅是很有助益的。

組別	動機	目標
激進分子（包括心懷不滿的員工）	• 聲譽受損 • 運營中斷	• 破壞資料 • 發佈敏感性資料 • 媒體關注 • 阻斷訪問資訊技術系統
罪犯	• 經濟利益 • 商業間諜活動 • 行業間諜活動	• 販賣偷來的數據 • 以被盜數據勒索贖金 • 以系統的可操作性勒索贖金 • 安排欺詐性的貨物運輸 • 為更複雜的犯罪收集情報（盜竊）
投機取巧者	• 挑戰/誇讚	• 突破網路安全防禦 • 經濟利益
國家/國家資助的組織/恐怖分子	• 政治利益 • 間諜	• 獲取知識 • 干擾經濟，破壞關鍵性的國家基礎設施

主要的風險

業務中斷

這可以說是與網路攻擊相關的最大風險。在涉及複雜業務活動的情況下，此類攻擊被證明具有極大的破壞性。阻斷服務及訪問客戶資訊、電子郵件系統、電話系統、互聯網、資訊資料庫、預定軟體、跟蹤軟體以及電子資料交換服務，很快就會造成嚴重的運營困難。對於有權訪問貴司系統的分包商與承租人，阻斷服務也可能造成負面影響。這項風險表明，制定強有力的業務連續性計畫是非常重要的。

成本

管理網路攻擊時，不可避免地會產生前期財務成本。無論是對電腦和系統進行更換或更新，還是為了克服面臨的挑戰而聘請專家提供協助，都需要不可預計的高昂前期成本投入。

經濟損失

許多無針對性網路攻擊的動機是敲詐錢財。攻擊者使用阻斷服務勒索軟體，以歸還對資訊技術服務的存取權限作為條件，向企業勒索贖金。付款授權網上欺詐也會給企業帶來巨大的經濟損失。

聲譽受損

貴司如遭到網路攻擊，毫無疑問會對貴司的客戶產生影響。這種影響可能是直接的，因為它會影響貴司在事件發生後立即提供服務的能力，甚至可能感染貴司客戶的系統。儘管克服網路攻擊的實際影響可能只需要幾天或幾周的時間，但對貴司造成的聲譽損害以及客戶對貴司的信心喪失，可能會持續多年。

智慧財產權的損失

企業的很多智慧財產權是通過數位技術保存的，範圍從機密的客戶資訊、商業敏感性資料到特定產品的資訊。網路攻擊導致的資訊盜竊是一個實實在在的威

相關法規

保護企業免受網路攻擊的國家級/區域級/國際法規正在不斷發展，例如：

- 《歐盟一般資料保護條例(GDPR)》 *https://ec.europa.eu/commission/priori- ties/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en*
- 《歐盟網路與資訊系統安全指令(NIS 指令)》 *https://www.ncsc.gov.uk/topics/nis-directive*
- 國際海事組織第 MSC.428(98)號決議 *http://www.imo.org/en/OurWork/Security/Guide_to_Mari- time_Security/Documents/Resolution%20MSC.428(98).pdf*

建議做法

國際海事組織（IMO）制定的法規框架，建議按照以下綱要要點處理網路攻擊風險：

- ❖ **識別：**定義員工在網路風險管理中的角色和職責，並識別如果受到干擾將對運營構成風險的系統/資產/資料/能力。
- ❖ **保護：**實施風險控制程式及應急計畫，防範網路事件發生，確保運營的連續性。
- ❖ **檢測：**開發與實施必要的活動，以儘快檢測到網路攻擊。
- ❖ **反應：**開發並實施為持續經營而提供必要恢復能力和還原必要系統的活動與計畫。
- ❖ **修復：**確定備份及恢復任何受影響運營活動所必需的系統的措施。在處理特定的風險敞口時應當採取積極主動的方法。

評估風險敞口

最近的案例突出表明，物流和貨運代理行業也未能倖免於網路攻擊。一旦發生網路攻擊，就有可能會對企業造成嚴重後果。因此，謹慎評估這項風險並做好相應準備是非常有必要的。

建議企業核查以下事項：

- ✓ 可能受到網路攻擊並因此出現運行漏洞的區域。

- 應對所有系統進行漏洞評估，以識別對業務至關重要的系統，並瞭解每個系統面臨的潛在風險以及受到網路攻擊時對整體業務連續性的影響。
- 企業應考慮對資訊技術（IT）系統和操作技術（OT）系統進行檢查。

  資訊技術系統是指用於資訊處理的技術，包括軟體、硬體和通訊軟體。而操作技術系統是指通過監控物理設備與程式用於探測或引起變化的硬體和軟體，存在於網路物理系統之中，包括射頻通信、導航系統、貨物處理和碼頭作業系統。
- 企業可參考 ISO/IEC TS 27008《資訊技術—安全技術—資訊安全控制評估指南》，該指南為現有控制措施提供了評估指南，以確保現有控制措施符合目的、有力並高效，而且與企業目標保持一致。
- 進行全面的威脅評估，以確定威脅總體情況並瞭解物流設施所面臨的潛在攻擊面。

✓ 是否已制定業務連續性計畫，以應對必須對攻擊做出回應時的情況。

✓ 是否已任命核心人員，負責資訊技術系統和操作技術系統的日常維護和網路攻擊的探測，並在遭遇攻擊時組建應急回應小組。

✓ 是否已對核心人員和員工進行妥當培訓，核心人員和員工是否瞭解他們在網路安全措施方面的責任，瞭解及時回應的責任，瞭解其在企業逐級上報程式中及時上報的責任（以便企業能在遭遇攻擊時及時回應）。

✓ 全體人員是否知曉、理解並遵守監管要求，以便保護業務。

✓ 是否投保了為公司業務提供一定程度保護的、適當的保險。

防範措施

雖然並非詳盡，企業可以考慮採用下列防範策略。建議企業首先考慮採用國家/國際相關技術標準，來建立相對較高的保護等級。而對於目前可能沒有足夠技術或財務能力的公司，建議採用一般防範措施。

- **採用下列資訊安全管理技術標準：**

1）ISO/IEC 27000- 系列
ISO/IEC 27000- 系列由國際標準組織（ISO）和國際電子電機委員會（IEC）發佈的資訊安全 管理系統（ISMS）標準組成。

該系列技術標準所載之管理系統規範，旨在通過明確管理控制實現資訊安全。該系列所載的有關資訊安全管理的最佳做法建議，有助於組織對資產（如財務資訊、智慧財產權、員工詳細資訊或協力廠商資訊）進行安全管理。

2）國家資訊系統標準

許多國家均制定有資訊系統技術標準，甚至針對物流企業制定了更加具體的技術標準。在實施這些標準時，企業可以向 FIATA 協會會員[1]、有關主管部門或技術專家尋求幫助。

- **採用一般防範措施：**

✓ 實施多級防禦，從最外層的物理安全開始，然後是管理級的程式和策略、防火牆和系統架構、電腦策略、帳戶管理和安全升級，最後是殺毒方案。

✓ 實施最小許可權原則，資訊和訪問限制採用“有必要知悉”原則。

✓ 採用網路加固措施，確保補丁管理充分並且受到積極審查。

✓ 採用隔離和協議感知過濾技術，防範可能影響關鍵系統的網路威脅。

✓ 採用可靠的可移動設備（例如 USB、筆記型電腦）策略，其規定應確保所有的 USB 在與其他設備一起使用前已經加密並通過病毒測試。

✓ 制定業務連續性計畫，從技術和商業的角度確定核心人員並建立程式，以防止網路攻擊的負面影響進一步擴大，並恢復企業運營。

✓ 經常組織安全意識簡介會及培訓專案，對所有員工進行最佳做法教育，教育內容包括安裝和維護軟體時如何避免感染和傳播，保護使用者資訊安全，以及如何應對協力廠商存在這類網路物理威脅。

✓ 對協力廠商供應商進行審查，以確保網路安全符合要求。

[1] FIATA 協會會員名單請見：https://fiata.com/home.html

拓展閱讀參考文件：

- 《船上網路安全指南》—波羅的海國際航運公會（BIMCO）https://www.bimco.org/news/priority-news/20181207-industry-publishes-improved-cyber- guidelines
- 《海上網路風險管理指南》—國際海事組織（IMO）http://www.imo.org/en/Our-Work/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx
- 《風險焦點：網路》—NYA、湯瑪斯米勒有限公司和聯運保賠協會

  https://www.ttclub.com/fileadmin/uploads/tt-club/Publications ment_store/UK_NYA_TT_Risk_Focus_-_Cyber_WEB.pdf