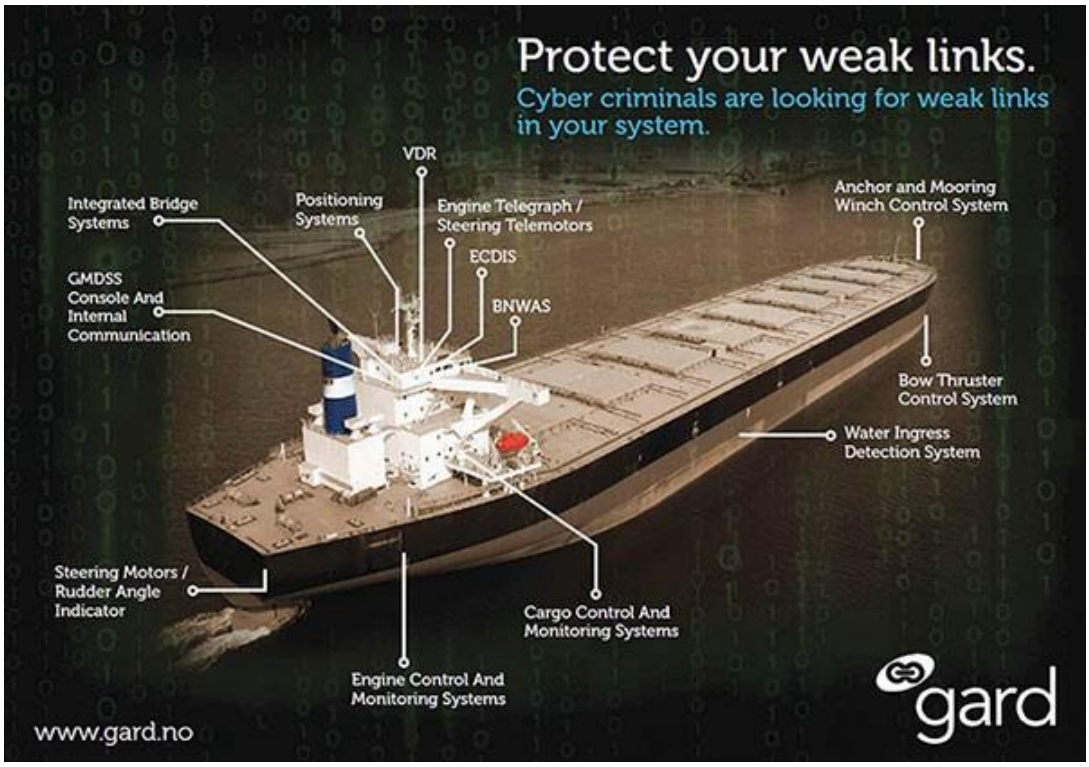
船上網路安全程序亟待加強

儘管國際海事組織規定，船東和經營人可以到 2021 年再將網路風險納入船舶安全管理體系，但網路犯罪分子已經著手實施犯罪。資料是一種資產，保護資料需要充分平衡保密性、完整性和可用性。網路安全不僅取決於船上系統和程序是如何設計的，還取決於它們是如何使用的——人為因素。



船東和經營人應當進行風險評估，並將應對網路風險的措施編入其船舶的安全管理體系（SMS）和船員意識培訓（如果還沒這麼做的話）。雖然國際海事組織規定，船東和管理人可以到 **2021 年 1 月 1 日**再將網路風險納入船舶安全管理體系，但接受石油公司國際海事論壇（OCIMF）船舶檢查報告程序審查的油船船東和經營人自 **2018 年 1 月 1 日**起，已經在其政策和程序中制定應對網路安全風險的內容了。

最新發佈的第三版行業網路風險管理指南《***船上網路安全指南***》介紹了將網路風險納入船舶安全管理體系的要求。該要求未被納入之前版本的指南中。本次納入該要求反映出業內對操作技術（OT）——比如導航系統和發動機控制機構——的風險評估有了更為豐富的經驗，同時也為應對海運供應鏈各方引起的船舶網路風險提供了更多指導。

網路風險可能不易識別

瞄準海運業、船舶及其船員的犯罪分子組織有序，並按照他們的運作方式不斷發展。這反映出網路風險在總體上不斷發展的本質。網路風險管理方法需對公司和船舶有針對性，但必須遵循相關國家、國際和船旗國法規要求的指導。

高級管理層應當將網路風險意識文化根植於船上的各級各部門，最終形成持續運作且通過有效的回饋機制不斷接受評估的靈活網路風險管理制度。

最新的網路安全調查顯示，業內對這一問題提高了認識，並已加強網路安全管理培訓，但仍有改進的空間。Futurenautics 集團開展的 2018 年船員互聯調查證實了這一點。根據該調查，僅有 15%的海員確認接受過網路安全培訓，僅有 33%的海員稱其服務的上一家公司有定期變更船上密碼的政策。

在 Gard，我們努力以最佳的方式保護我們會員和客戶的利益。我們的建議是全方位應對網路風險，通過程序、技術、以及最為重要的人員等方面的措施保護 IT 和 OT 系統的保密性、完整性和可用性。網路犯罪分子獲取訪問權最簡單和最常用的方法就是通過疏忽大意或缺乏培訓的個人。

建議 1：關注政策、程序和風險評估

最新的《船上網路安全指南》預期，網路事件會帶來實體影響，導致潛在的安全和/或污染事件。因此公司不僅需要評估使用船上 IT 設備產生的風險，還要評估使用船上 OT 設備產生的風險，同時要確立適當的保護措施，防範涉及 IT 或 OT 設備的網路事件。

公司的網路風險管理計畫和程序必須與公司政策中 ISPS 章程和 ISM 章程規定的現有保安和安全風險管理要求保持一致。關鍵網路系統培訓、操作和維護的相關要求也應被納入船上相關文檔。

國際海事組織海上安全委員會（MSC）於 2017 年 6 月通過了有關*安全管理體系之海上網路風險管理*的 MSC.428(98)號決議。該決議規定，最晚在 2021 年 1 月 1 日之後對公司符合證明的首次年度審核時，網路風險管理應按照 ISM 章程的宗旨和要求，納入經核准的安全管理體系。

符合證明的持證人對確保船上網路風險管理負有最終責任。如果船舶由第三方管理，建議船舶管理人與船東就誰對該事項負責達成協議。雙方應當強調責任分配、務實期望調整、有關給管理人具體指示的約定、參與採購決策的可能性以及預算要求。

除了 ISM 要求以外，該等協議還應考慮其他適用法律，比如《歐盟通用資料保護法規》（GDPR）或其他沿海國家的特別網路法規。管理人和船東應考慮以這些準則為基礎，

開誠佈公地討論如何最好地實施有效的船上網路風險管理制度。有關網路風險管理責任的任何協定應當以書面正式做出。

公司還應在服務供應商的協定和合同中評估並規定供應商的實體安全與網路風險管理程序。同樣地，協調船舶掛靠港口的工作，由於在本質上同時涉及全球和當地因素，因此也非常複雜。這包括從代理處獲得最新情況，協調各港口供應商的資訊，港口國管制，處理船舶和船員要求，以及船舶、港口和岸上當局的電子溝通。

代理的品質標準很重要，因為像其他行業一樣，代理也是網路犯罪分子的目標。電子轉帳欺詐、虛假船舶指定等網路犯罪，以及勒索軟體、駭客等網路威脅需要船東和代理之間有共同的網路戰略和憑藉網路增強的相互關係，從而緩解這些風險。

建議 2：確保系統設計和配置是安全的，且可以被充分理解和遵循

程序的問題在於好的想法可能停留於紙面上。因此重要的是，要確保執行涉及網路安全任務的人員理解，相關程序的目的是為了防止未經授權的訪問，而不是簡單地滿足規則制定者或其直接上級的要求。

與有過往例證可查的其他安全和保安領域不同，由於缺乏有關事件及其影響的事實，網路風險管理更具挑戰性。在掌握這樣的例證之前，攻擊的規模和頻率將繼續不得而知。

航運業以及金融機構、公共管理和航空運輸等其他行業的過往經驗表明，網路攻擊一旦得逞，可能導致嚴重的服務中斷。

現代技術可能會使船舶的漏洞增多，特別是在網路不安全和可隨意訪問互聯網的情況下。此外，岸上和船上人員可能並不知道有些設備製造商可以遠端訪問船上設備及其網路系統。作為風險評估的重要組成部分，應當將作業船舶受到的不明、非協調遠端訪問情況納入考慮範圍。

Gard 建議公司充分瞭解船舶的 IT 和 OT 系統，以及這些系統是如何與岸側（包括公共當局、海運碼頭及裝卸公司）連通和集成的。這需要瞭解船上所有基於電腦的系統以及網路事件是如何危害安全、操作和業務的。

有些 IT 和 OT 系統可以遠端訪問，並且可以持續連接互聯網進行遠端監控、資料收集、維護和安全保護。這些系統可能是“第三方系統”，由承包商從遠端位置對系統進行監控和維護，其有可能允許雙向數據流，也有可能只允許上傳資料。

舉例而言，具有遠端控制、訪問或配置功能的系統和工作站可以是：

- 船舶行政管理網路內的駕駛台和機艙電腦以及工作站
- 配備冷藏溫度控制系統的集裝箱等貨物或可遠端追蹤的特殊貨物

- 穩性決策支援系統
- 船體應力監測系統
- 導航系統，包括電子海圖（ENC）和航行資料記錄儀（VDR）
- 動態定位系統（DP）
- 貨物裝卸和積載系統，發動機系統，以及貨物管理和裝載計畫系統
- 安全和保安網路，例如 CCTV（閉路電視）
- 鑽井作業、防噴器、海底安裝系統等專業系統
- 液化氣體船、海底電纜安裝和修理用緊急停車系統。

以下是現有船舶以及一些新建船上常見的網路漏洞：

- 作業系統過時及不受支援
- 防毒軟體以及惡意軟體防護過期或缺失
- 未採取適當的安全配置和最佳做法，包括無效的網路管理以及使用預設的管理員帳戶和密碼
- 船上電腦網路缺乏邊界保護措施和網路分段
- 對保證安全起關鍵作用的設備或系統始終與岸側相連接
- 對第三方（包括承包商和服務供應商）的訪問控制不足。

建議 3：提供適當的船上意識教育和培訓

當今，網路安全中最薄弱的環節是人為因素。因此，通過給予海員適當的培訓，來說明其識別和報告網路事件，具有重要意義。

在評估網路風險時，應同時考慮外部和內部的網路威脅。船上人員對保護 IT 和 OT 系統起著關鍵作用，但他們也可能疏忽大意，比如他們可能使用可移動介質在系統之間傳輸資料，而未採取預防措施來防止惡意軟體的轉移。培訓和意識教育應根據包括船長、高級船員、普通船員在內的船上人員的資歷量身定制。

Gard 定期發佈案例，供安全會議上研究討論，重點關注風險評估程序以及引發事故的一系列過錯的識別。其中一則案例研究就涉及與船員相關的網路安全。我們鼓勵船長將該**案例研究**編入培訓內容，供船上高級船員和普通船員比較、分析和討論。

Gard 在網路安全意識方面的宣傳舉措

根據我們對網路安全案例的分析，Gard 和 DNV GL 製作了一段**防損意識視頻**和一份演示文稿，其中對海運業如何解決該問題提出了一些建議。這些資料並不旨在宣導行業變革或規則變更，而是建議改變人們的行為方式。

以下連結將帶您進入我會的網路安全意識宣傳網站，該網站包含網路安全方面的視頻、一則案例研究以及其他防損資料：http://www.gard.no/web/content/cyber-security-awareness-information-package。

作者：**Jarle Fosen**
防損主管，阿倫達爾