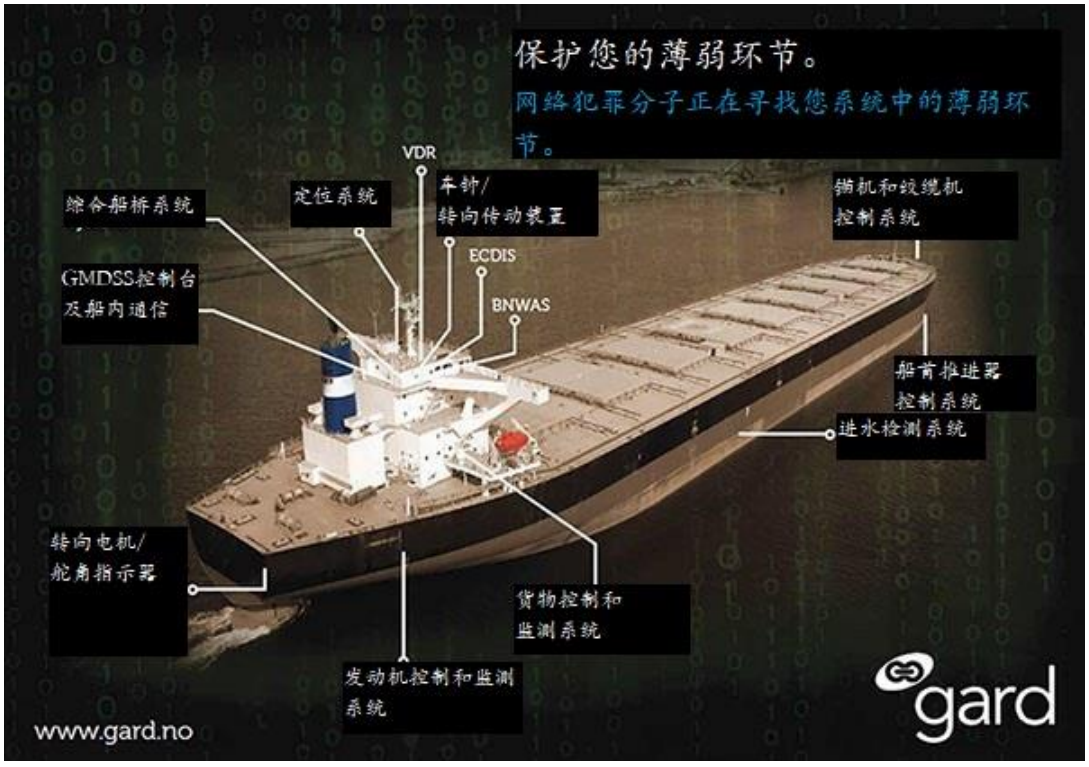
船上网络安全程序亟待加强

尽管国际海事组织规定，船东和经营人可以到 2021 年再将网络风险纳入船舶安全管理体系，但网络犯罪分子已经着手实施犯罪。数据是一种资产，保护数据需要充分平衡保密性、完整性和可用性。网络安全不仅取决于船上系统和程序是如何设计的，还取决于它们是如何使用的——人为因素。



船东和经营人应当进行风险评估，并将应对网络风险的措施编入其船舶的安全管理体系（SMS）和船员意识培训（如果还没这么做的话）。虽然国际海事组织规定，船东和管理人可以到 **2021 年 1 月 1 日**再将网络风险纳入船舶安全管理体系，但接受石油公司国际海事论坛（OCIMF）船舶检查报告程序审查的油船船东和经营人自 **2018 年 1 月 1 日**起，已经在其政策和程序中制定应对网络安全风险的内容了。

最新发布的第三版行业网络风险管理指南《***船上网络安全指南***》介绍了将网络风险纳入船舶安全管理体系的要求。该要求未被纳入之前版本的指南中。本次纳入该要求反映出业内对操作技术（OT）——比如导航系统和发动机控制机构——的风险评估有了更为丰富的经验，同时也为应对海运供应链各方引起的船舶网络风险提供了更多指导。

网络风险可能不易识别

瞄准海运业、船舶及其船员的犯罪分子组织有序，并按照他们的运作方式不断发展。这反映出网络风险在总体上不断发展的本质。网络风险管理方法需对公司和船舶有针对性，但必须遵循相关国家、国际和船旗国法规要求的指导。

高级管理层应当将网络风险意识文化根植于船上的各级各部门，最终形成持续运作且通过有效的反馈机制不断接受评估的灵活网络风险管理制度。

最新的网络安全调查显示，业内对这一问题提高了认识，并已加强网络安全管理培训，但仍有改进的空间。Futurenautics 集团开展的 2018 年船员互联调查证实了这一点。根据该调查，仅有 15%的海员确认接受过网络安全培训，仅有 33%的海员称其服务的上一家公司有定期变更船上密码的政策。

在 Gard，我们努力以最佳的方式保护我们会员和客户的利益。我们的建议是全方位应对网络风险，通过程序、技术、以及最为重要的人员等方面的措施保护 IT 和 OT 系统的保密性、完整性和可用性。网络犯罪分子获取访问权最简单和最常用的方法就是通过疏忽大意或缺乏培训的个人。

建议 1：关注政策、程序和风险评估

最新的《船上网络安全指南》预期，网络事件会带来实体影响，导致潜在的安全和/或污染事件。因此公司不仅需要评估使用船上 IT 设备产生的风险，还要评估使用船上 OT 设备产生的风险，同时要确立适当的保护措施，防范涉及 IT 或 OT 设备的网络事件。

公司的网络风险管理计划和程序必须与公司政策中 ISPS 规则和 ISM 规则规定的现有保安和安全风险管理要求保持一致。关键网络系统培训、操作和维护的相关要求也应被纳入船上相关文件。

国际海事组织海上安全委员会（MSC）于 2017 年 6 月通过了有关*安全管理体系之海上网络风险管理*的 MSC.428(98)号决议。该决议规定，最晚在 2021 年 1 月 1 日之后对公司符合证明的首次年度审核时，网络风险管理应按照 ISM 规则的宗旨和要求，纳入经核准的安全管理体系。

符合证明的持证人对确保船上网络风险管理负有最终责任。如果船舶由第三方管理，建议船舶管理人与船东就谁对该事项负责达成协议。双方应当强调责任分配、务实期望调整、有关给管理人具体指示的约定、参与采购决策的可能性以及预算要求。

除了 ISM 要求以外，该等协议还应考虑其他适用法律，比如《欧盟通用数据保护法规》（GDPR）或其他沿海国家的特别网络法规。管理人和船东应考虑以这些准则为基础，

开诚布公地讨论如何最好地实施有效的船上网络风险管理制度。有关网络风险管理责任的任何协议应当以书面正式做出。

公司还应在服务供应商的协议和合同中评估并规定供应商的实体安全与网络风险管理程序。同样地，协调船舶挂靠港口的工作，由于在本质上同时涉及全球和当地因素，因此也非常复杂。这包括从代理处获得最新情况，协调各港口供应商的信息，港口国管制，处理船舶和船员要求，以及船舶、港口和岸上当局的电子沟通。

代理的质量标准很重要，因为像其他行业一样，代理也是网络犯罪分子的目标。电子转账欺诈、虚假船舶指定等网络犯罪，以及勒索软件、黑客等网络威胁需要船东和代理之间有共同的网络战略和凭借网络增强的相互关系，从而缓解这些风险。

建议 2：确保系统设计和配置是安全的，且可以被充分理解和遵循

程序的问题在于好的想法可能停留于纸面上。因此重要的是，要确保执行涉及网络安全任务的人员理解，相关程序的目的是为了防止未经授权的访问，而不是简单地满足规则制定者或其直接上级的要求。

与有过往例证可查的其他安全和保安领域不同，由于缺乏有关事件及其影响的事实，网络风险管理更具挑战性。在掌握这样的例证之前，攻击的规模和频率将继续不得而知。

航运业以及金融机构、公共管理和航空运输等其他行业的过往经验表明，网络攻击一旦得逞，可能导致严重的服务中断。

现代技术可能会使船舶的漏洞增多，特别是在网络不安全和可随意访问互联网的情况下。此外，岸上和船上人员可能并不知道有些设备制造商可以远程访问船上设备及其网络系统。作为风险评估的重要组成部分，应当将作业船舶受到的不明、非协调远程访问情况纳入考虑范围。

Gard 建议公司充分了解船舶的 IT 和 OT 系统，以及这些系统是如何与岸侧（包括公共当局、海运码头及装卸公司）连通和集成的。这需要了解船上所有基于计算机的系统以及网络事件是如何危害安全、操作和业务的。

有些 IT 和 OT 系统可以远程访问，并且可以持续连接互联网进行远程监控、数据收集、维护和安全保护。这些系统可能是“第三方系统”，由承包商从远程位置对系统进行监控和维护，其有可能允许双向数据流，也有可能只允许上传数据。

举例而言，具有远程控制、访问或配置功能的系统和工作站可以是：

- 船舶行政管理网络内的驾驶台和机舱计算机以及工作站
- 配备冷藏温度控制系统的集装箱等货物或可远程追踪的特殊货物

- 稳性决策支持系统
- 船体应力监测系统
- 导航系统，包括电子海图（ENC）和航行数据记录仪（VDR）
- 动态定位系统（DP）
- 货物装卸和积载系统，发动机系统，以及货物管理和装载计划系统
- 安全和保安网络，例如 CCTV（闭路电视）
- 钻井作业、防喷器、海底安装系统等专业系统
- 液化气体船、海底电缆安装和修理用紧急停车系统。

以下是现有船舶以及一些新建船上常见的网络漏洞：

- 操作系统过时及不受支持
- 防病毒软件以及恶意软件防护过期或缺失
- 未采取适当的安全配置和最佳做法，包括无效的网络管理以及使用默认的管理员帐户和密码
- 船上计算机网络缺乏边界保护措施和网络分段
- 对保证安全起关键作用的设备或系统始终与岸侧相连接
- 对第三方（包括承包商和服务供应商）的访问控制不足。

建议 3：提供适当的船上意识教育和培训

当今，网络安全中最薄弱的环节是人为因素。因此，通过给予海员适当的培训，来帮助其识别和报告网络事件，具有重要意义。

在评估网络风险时，应同时考虑外部和内部的网络威胁。船上人员对保护 IT 和 OT 系统起着关键作用，但他们也可能疏忽大意，比如他们可能使用可移动介质在系统之间传输数据，而未采取预防措施来防止恶意软件的转移。培训和意识教育应根据包括船长、高级船员、普通船员在内的船上人员的资历量身定制。

Gard 定期发布案例，供安全会议上研究讨论，重点关注风险评估程序以及引发事故的一系列过错的识别。其中一则案例研究就涉及与船员相关的网络安全。我们鼓励船长将该**案例研究**编入培训内容，供船上高级船员和普通船员比较、分析和讨论。

Gard 在网络安全意识方面的宣传举措

根据我们对网络安全案例的分析，Gard 和 DNV GL 制作了一段**防损意识视频**和一份演示文稿，其中对海运业如何解决该问题提出了一些建议。这些资料并不旨在倡导行业变革或规则变更，而是建议改变人们的行为方式。

以下链接将带您进入我会的网络安全意识宣传网站，该网站包含网络安全方面的视频、一则案例研究以及其他防损资料：http://www.gard.no/web/content/cyber-security-awareness-information-package。

作者：Jarle Fosen

防损主管，阿伦达尔