全球大流行病中的网络安全问题

虽然国际海事组织（IMO）已经敦促船东和船舶营运人在 2021 年前将网络风险纳入船舶安全管理体系，但网络罪犯早已悄然而至。尤其在新冠病毒这样的全球大流行病的危机下，不怀好意的网络罪犯往往会乘机通过各种恶意的方法来获取利益。

为解决“拒绝物理访问”、“船舶被隔离”和“旅行限制”等实务操作上的问题，船东目前正在积极开放远程访问，对船舶使用远程数字勘察工具，并鼓励岸上人员在家远程工作。

同时，公司还越来越多地使用移动设备访问船舶上的操作系统和核心业务系统。在这种状况下，未受保护的设备可能导致数据丢失、隐私泄露和系统被劫持的风险。因此切实保护作为宝贵资产的数据需要在机密性、完整性和实用性之间保持良好的平衡。

在一个遍布网络的时代，随着更多的技术改造、“云”技术的广泛使用，以及更普及的船舶联网能力，使得安全威胁不断增加。网络罪犯将以高度复杂的方式同时攻击操作系统和备份能力，以造成有破坏性的网络攻击。网络安全不仅取决于公司和船上的系统和流程是怎样设计的，还取决于它们如何被使用——即人的因素。

网络风险可能不易识别

基于行业特点，航运业中船舶及其船员的组织合作良好，且运作方式在不断优化，但网络犯罪分子对此是虎视眈眈。这总体上也反映了网络风险不断演变的本质。网络风险管理方法应当是基于公司和船舶，但也必须遵循相关国家、国际和船旗国法规中的要求。

对于还未做好应对的船东和船舶营运人，应首先进行风险评估，同时把应对网络风险的措施纳入其船舶安全管理体系（SMS）和船员意识培训里。船东和船舶营运人还应将网络风险意识文化融入公司和船上

的各级部门。其目的是为营造一个灵活的网络风险管理制度，以确保制度体系才能持续运作，并能通过有效的反馈机制不断进行评估改进。

大部分船级社以及若干海事咨询公司都发布过关于船舶网络安全的指南和建议。船级社作为船旗国当局认可的组织，现在也可以进行包括网络风险在内的 ISM 审核。

船级社还提供了一套基于自愿原则的网络安全船级理念，以应用于验证安全船舶的设计和操作，以及网络安全类型的认证，来支持制造商使用网络安全系统和组件。船级社作为顾问，还可以为船上和办公室提供网络安全风险评估、改进、渗透测试和培训支持。

在 Gard，我们努力通过最佳途径保护会员和客户的利益。我们的建议是对网络风险采取全面的方法，通过涵盖流程、技术和最重要的人员的措施，保护 IT 和 OT 系统的机密性、完整性和可访问性。对于网络犯罪分子来说，最容易又最常见的入侵目标，就是通过疏忽大意或缺乏训练的个人。

建议 1：专注于政策、流程和风险评估

最新的船舶网络安全指南 预计，网络事故会对现实产生影响，并导致潜在的安全以及污染事件。因此，公司不仅需要评估 IT 设备的使用所带来的风险，还需要评估船上 OT 设备的使用所带来的风险，并建立适当的防范措施，防止其中任何一种可能带来的网络事故影响。

公司的网络风险管理计划和流程，必须与公司政策里 ISPS 和 ISM 规范中的现有安保和安全风险管理要求保持一致。关键网络系统的培训、操作和维护的相关要求也应包含在船上的相应文件中。

国际海事组织海事安全委员会（MSC）于 2017 年 6 月通过了关于*安全管理体系中海事网络风险管理*的 MSC.428(98)号决议 。决议规定，经批准的安全管理体系应包括符合 ISM 准则目标和要求的网络风险管理，且不得迟于 2021 年 1 月 1 日，对公司合规性文件的首次年度验证。

基于 MSC-FAL.1/Circ.3《海上网络风险管理指南》中的建议，该决议确认，应采用现有的风险管理做法，解决因日益依赖网络系统而产生的运营风险。该指南规定了以下可采取的行动来支持有效的网络风险管理：

1.***识别***：定义负责网络风险管理的角色，识别系统、资产、数据和能力，评估如果它们被中断时将对船舶运营构成的风险。
2.***保护***：实施风险管控流程、措施和应急计划，以防止网络事故，并确保航运业务运作的连续性。
3.***检测***：制定并实施能及时检测网络事故所需的流程和防御措施。
4.***响应***：制定和实施有恢复能力的活动和计划，以恢复因网络事故而中断的航运业务或服务所需的系统。
5.***恢复***：确定如何备份和恢复受网络事件影响的航运业务所需的网络系统。

DOC 证书持有人是确保船上网络风险管理的最终负责人。由第三方管理船舶时，建议船舶管理人与船东协商好责任归属。双方都应重视责任划分，确定符合实际的预期、对船舶管理人的具体指示达成一致。尽可能参与采购决策以及预算要求的制定。

除 ISM 体系要求外，此类协议还应考虑其他适用法律，如欧盟《通用数据保护条例》（GDPR）或其他沿海国家的特定网络条例。船舶管理者和船东应考虑将这些指南作为基础，以公开讨论如何最好地实施有效的网络风险管理制度。任何有关网络风险管理责任的协议都应是正式的和书面的。

公司还应在供应商协议和合同中，涵盖并评估服务供应商的物理安全和网络风险管理流程。同样，协调船舶挂靠港口是一项非常复杂的任务，包含了全球性和地方性诸多特性。其中包括船舶代理的消息更

新、与所有港口供应商的协调信息、港口国管制、处理船舶和船员的要求，以及船舶、港口和岸上机构之间的电子通信等多方面的工作。

另外，船舶代理的选定的质量标准十分重要，因为和所有其他企业一样，代理商也是网络罪犯的目标。网络犯罪：如电子电信欺诈和虚假船舶预约，以及网络威胁：如勒索软件和黑客攻击，都要求船东和代理人双方采取协同的网络战略并加强彼此之间的网络关系，来减轻这些风险。

建议 2：确保系统设计和配置的安全性、并被贯彻理解和执行

程序的问题在于，良好的意图可能会变成纸上谈兵。因此，如何确保负责执行涉及网络安全任务的人员，充分了解该等程序的目的是防止未经授权的访问，而非仅仅是应对监管机构或其直接上级的要求就变得尤为重要。

与传统的可参照过往经验的安全/安保领域不同，网络风险管理由于缺乏相关事故的事实和影响而变得更具挑战性。在我们掌握有关证据之前，网络攻击的规模和频率都往往未知的。

航运业和其他商业部门（如：金融机构、公共管理部门和航空运输）的经验表明，既遂的网络攻击可能导致由于服务无法正常运转而造成的重大损失。

现代科技带来便利的同时也可能会给船舶管理增加漏洞，特别是当船舶置于不安全的网络之中，并被允许自由访问船舶的互联网。此外，岸上和船上人员可能没有意识到一些设备制造商保留和维持了对船舶相关设备和网络系统的远程登陆访问权限。对于船舶而言，对不明且不协调的远程登陆权限的管理应该是风险评估的一个重要部分。

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上连接和整合的（包括公共当局、海事码头和装卸工）。这需要对船上所有基于计算机的系统，以及网络事故如何危及安全、运营和业务进行了解。

一些 IT 和 OT 系统可以远程访问，并且可能持续连接互联网，进行关联远程监控、数据收集、维护、安全和安保。这些系统可以是“第三方系统”，因此承包商可以在远程位置监控和维护系统，并且可以是双向数据流或仅上传数据。

具有远程控制、访问或配置功能的系统和工作站包含以下几种：

- 船舶舰桥和机舱计算机以及船舶行政网络上的工作站，
- 带冷藏温度控制系统的集装箱或可远程跟踪的特化货物，
- 稳定性决策支持系统
- 船体应力监测系统
- 导航系统，包括电子导航图（ENC）航行数据记录器（VDR）
- 动态定位系统（DP）
- 货物装卸和存放、发动机、货物管理和装载计划系统
- 安全和安保网络，如闭路电视（CCTV）
- 专业系统，如钻井作业、防喷器、海底安装系统,
- 油轮紧急关闭（ESD），海底电缆安装和维修

以下是一些常见的网络漏洞，可能在现有船舶和一些新造船舶上出现：

- 淘汰且不受维护的操作系统，
- 淘汰或已缺失防病毒，防恶意攻击的软件，
- 安全配置和正确操作不足，包含无效的网络管理和使用默认的管理员帐户和密码，

- 船载计算机网络缺乏边界保护措施和网络划分。
- 安全关键设备或系统始终与岸上连接。
- 缺乏对包括承包商和服务提供商在内的第三方的访问控制。

建议 3：提供恰当的船上安全防范意识和培训

当前，网络安全最薄弱的环节仍然是人为因素。因此，对船员进行适当培训，帮助他们识别和报告网络事件十分重要。

最新的网络安全调查显示，业界对这一问题的认识有所提高，并增加了网络风险管理培训，但仍有改进的空间。这一点也得到了 Futurenautics Maritime 集团与其合作伙伴进行的“2018 年船员连通性调查”的证实，只有 15%的海员表示接受过网络安全培训，且仅有 33%的海员表示，他们最近一间工作的公司有定期更改船上密码的政策。

在评估网络风险时，外部和内部网络威胁都应当加以综合考虑。船上人员在保护 IT 和 OT 系统方面起着关键作用，但疏忽大意在所难免，例如：使用可移动媒体端在系统之间传输数据时不采取防止恶意软件传输的措施。培训和培养意识应根据包括船长、高级船员和普通船员在内的船上人员进行程度的调整。

Gard 此前曾与 DNV-GL 一起发布了一个免费下载和分享的网络安全意识活动，针对日常工作和日常事务，为“普通人”揭开网络问题的神秘面纱，并建立和培养船员和其他人的相关素质和能力。此等行动的目的并不是为了改变任何行业规则，而旨在改变人们的行动和行为方式。

最后，我们建议每个人保持网络警惕，避免所有有关“COVID-19”钓鱼程序：

- 要谨慎处理任何包含“COVID-19”相关的主题行、附件或超链接的电子邮件，并小心与 COVID-19 相关的社交媒体请求、文本或电话。
- 使用可靠的资源—比如来自合法的政府网站的最新的，基于事实的网络安全和 COVID-19 信息
- 不要在电子邮件中透露个人或财务信息，也不要回复此类信息的邮件请求。
- 请谨记在完成工作后，断开或关闭任何外部端口的临时远程访问。

More resources

Gard

August 2019 - Maritime industry targeted by cyber criminals

July 2019 - Ship operators cannot afford to turn a blind eye to cyber security

Jan 2019 - Denmark identifies cyber threats in its maritime sector

December 2018 - It is time to strengthen your onboard cyber security procedures

June 2018 – Cyber security awareness campaign

Full 20 mins video for crew awareness and training (MP4 - 635Mb)

Short 3 mins teaser of the full video for creating interest (MP4 - 102Mb)

Loss Prevention Poster Cyber security

Loss Prevention Poster Think before you click

Loss Prevention Poster Is your download free of malware?

BIMCO

BIMCO together with the International Chamber of Shipping (ICS) have, October 2019, published a new "Cyber Security Workbook for On Board Ship Use" meant to serve as a guide for the master and officers on board ships and thereby help them prepare for a potential cyber incident.

BIMCO together with Safety at Sea publish a cyber security white paper, in September 2019, containing advice based on results and findings from Cyber Security Surveys produced over the last four years, as well as on feedback and knowledge from experts at roundtable events.

BIMCO together with other leading shipping organisations have in August 2019, published version 3.0 of the Guidelines on Cyber Security onboard Ships (commonly referred to as the BIMCO Guidelines), which offer guidance to shipowners and operators on how to assess their operations and develop the necessary procedures and actions to improve resilience and maintain integrity of cyber systems onboard their ships. The guidelines have been aligned with the recommendations given in the IMO Guidelines on Cyber Risk Management. See also this useful poster which can help prevent the most common cyber incidents.

US Coast Guard

The US Coast Guard published its *Cyber Strategy* in July 2015 in response to what it perceives is one of the greatest threats to US economic and national security interests. The Coast Guard's cyber security website provides access to the strategy document and other cyber-related information, e.g. their *Cyber Maritime Bulletins*, and can be viewed by using the link: *http://homeport.uscg.mil* and the following path: Missions > Cybersecurity

The US Coast Guard published version 3 of its Guidelines for Cybersecurity Onboard Ships on 13 December 2018. These guidelines were developed to mitigate the potential safety, environmental, and commercial consequences of a cyber incident and are designed to assist companies in formulating their own approaches to cyber risk management onboard ships.

UK Department of Transport (DfT)

The DfT published its Code of Practice: Cyber Security for Ships on 13 September 2017, providing a management framework that can be used to reduce the risk of cyber incidents that could affect the safety or security of a ship, its crew, passengers or cargo. The Code of Practice is intended to be used together with DfT's Good practice guide: cyber security for ports and port systems, latest edition issued on 27 January 2020.

Although the Code of Practice refers to Maritime Security Regulations in the UK, its provisions are complementary to those of the SOLAS Convention, the ISM Code and

the ISPS Code and it is therefore considered as a useful guidance document for all nationalities of ships.

Classification Societies

ABS Cyber insight: A Simple approach to understanding cyber risk in OT assets

ABS Cyber insight: Cyber Security Solutions for Operational Technology

ABS Application of Cybersecurity Principles to Marine and Offshore Operations - CyberSafety Volume 1

DNV GL Maritime cyber security insight (including ISM guidance)

DNV GL Recommended practice: Cyber security resilience management

Lloyd's Register Cyber insight - Tackling an evolving threat

Lloyd's Register Procedure for the Assessment of Cyber Security for Ships and Ships Systems

作者：Jarle Fosen

高级防损主管