ARTICLE

NORTH
SERVICE, STRENGTH, QUALITY

应对网络犯罪 行动不容迟疑

勉勉强强总算有一个月没有听闻知名企业和政府部门遭受网络攻击的最新案例了。网络犯罪现已迅速成为影响所有行业的全球性威胁，而近期关于马士基终端瘫痪的报道表明：海运供应链同样未能幸免。

网络威胁是真实存在的，并且会严重扰乱航运业务。最新的发展形势说明航运企业必须采取措施去改善他们的网络安全。

网络风险与ISM Code

国际海事组织海事安全委员会（MSC）已经确认网络风险应当被纳入ISM Code的体系管理。

一段时间以来，很多主管机关已经开始担心航运业在网络风险方面的管控能力不够坚固，并鼓励航运企业自主地建立起网络安全管理体系。此最新发展使得船东必须通过他们的安全管理体系来应对网络风险。

MSC428(98)号决议要求一个被认证批注的安全管理体系应当考虑网络风险管理，并鼓励相关主管机关在2021年1月1日以后第一次公司年审符合声明（Document of Compliance）时确保网络风险已经在安全管理体系中被妥善应对。

TMSA 3

网络风险管理现已纳入到了《油轮船舶管理与自评第三版》（TMSA 3）中，具体到第七条“应对改变”和第十三条“海事安全”。

在第七条3.3款的关键绩效指标中，网络安全已经作为最佳实务操作指南的一部分被列明为软件管理责任中的一项。而第十三条则明确指出，应当把网络安全作为一项会动摇安全性的威胁而加以应对。

显然，石油行业已经意识到油轮船东们需要行动起来，而且还通过TMSA3这一渠道从商业驱动的角度来鼓励全行业一同参与。油轮船东和租家们，时不我待了。

一项艰巨的任务？

网络安全的应对让许多航运企业有点望而生畏。这是一个新型的课题，涉及到一些无法完全理解的内容，而且大多数人至今未接受过针对此类风险的正式培训。但我们的优势是，航运公司将非常熟悉国际海事组织对于船舶网络安全的风险管控和行业指南里所建议的风险管理框架，同时，我们还可以利用行业其他板块在落实网络安全系统中获取的经验。

NORTH OF ENGLAND MARINE CONSULTANTS (SHANGHAI) LTD CO. Room 302, Building 7, 18 Gongping Road, Hongkou District, Shanghai 200082 P.R. China
Tel: +86 21 6087 5988 Facsimile: +86 21 6087 6198 Email: Shanghai.marine@nepia.com
Website: www.nepia.com

2021年近在眼前，网络安全风险渗透着航运公司运作的每个环节。要识别探测风险和漏洞，并采取措施应对网络安全的威胁，非一日之功且任重而道远。是时候要行动起来了。

不要拖延，现在就行动

北英保赔协会在提升网络安全意识方面已有时日—你可以在以下链接，我们的视野(Insights)栏目内了解更多关于网络安全的信息，或者直接点击左下方“阅读原文”获取详情。

http://www.nepia.com/insights/cyber-security/