August 2017. Issue 229 in the series

TT Talk 第229期

1. 运输链中的电子风险
2. 网络经验教训：应两手抓
3. 法律焦点之电放问题思考

1. 运输链中的电子风险

从事国际运输行业的人几乎没有不知道2017年6月底发生的“NotPetya”网络攻击事件（源自类似Petya的全新形式勒索病毒，可以将硬盘整个加密和锁死，从内存或者本地文件系统里提取密码）。该事件应引起各组织对每一个由网络活动所引发的风险评估，进行复审。

网络风险早已不是一个“是否会发生”的问题，而是“何时会发生”的问题。所以现在每一个企业要面临的是，更为紧迫地完成全面彻底的风险评估任务。也许最大的问题就在于这是一个新的模式，而既有的或以往的模式可能是不足够的。网络风险巨大、复杂、多样，且大部分不为人知，但它有能力从根本上影响一个企业的运营。

不甚满意的现状

现状有两方面令人不甚满意：首先，全球性企业所使用的相连接的基础设施在本质上并不安全，其次，人类的天性和才智可能是最强大的防护力量但也是最大的弱点。如果有人不相信“正义”与“邪恶”的斗争在这个舞台上的激烈程度，那么7月底由黑客发动的“#LeakTheAnalyst”（已成为推特上的热搜词汇）运动应该已敲响了警钟。

我们应考虑到对广为传播的WannaCry病毒和NotPetya网络攻击事件的防护不能仅停留在技术层面，尽管这方面非常重要。很显然，两个病毒都属于加密的勒索软件，攻击目标为常用的Windows操作系统。感染的方式通常是分发的电子邮件内含有恶意链接，且通常来自一个未知的发件人。一旦企业的内部网络触发病毒，那么勒索软件可以迅速传播并感染其他易受攻击的设备、服务器和系统。

“应考虑到对广为传播的WannaCry病毒和NotPetya网络攻击事件的防护不能仅停留在技术层面”

在大多数情况下，可以假设许多企业成为不知情的受害者，虽然商业间谍之类的情况不能完全忽视。但最近发生的事件，其影响已遍及全球，侵害了广泛的行业，包括食品公司、律师事务所、航运业、银行业、以及公用事业和医疗行业。简单的结论就是犯罪分子寻找利用一切所能发现的弱点，来勒索企业钱财并造成重大破坏。

运输链暴露的问题

令人惊讶的是多式联运行业，虽然并没有在这次席卷全球的网络攻击中遭受过多的曝光和破坏。这可能是由于在某种程度上事故公开透明度较低、报道少；现有的传闻表明，许多利益相关方是持续不断且各种类型攻击下的主要对象。可以理解的是，企业通常对于网络犯罪活动的发生和方式采取遮遮掩掩的态度；而A P Möller公司保证从最近的事件中吸取教训，其态度是值得首肯的。

在现实中，多式联运业暴露的风险有其独特性，因为它是越来越依赖连接不同国家中的每一个独立企业内的信息和通信技术（ICT），与不同的第三方利益相关方互动，且经常使用定制/专有的应用程序，其安全协议可能不会提示最近的安全漏洞。除了这些，在当前的经济和竞争环境下，许多企业会建立除网络风险外的综合风险偏好，将稀缺的预算放在优先考虑的问题上。

“许多企业会建立除网络风险外的综合风险偏好”

由此造成的影响是巨大的，范围包括简单的偷盗或诈骗，以及潜在地对系统、设备的控制或操纵，并延伸到数据或知识产权的泄露。

与人类接触的病毒一样，基本的保护课程一般都是众所周知的，其中包括：

- 确保软件补丁定期应用，现在可能已认识到没有时间来评估相关应用程序的间接影响；

- 保持运行有效的防病毒软件和强劲的垃圾邮件过滤系统（大多数供应商会迅速针对进化的恶意软件病毒提高检测能力）；和
- 系统地定期备份关键数据，包括确保备份文件离线存储，从而不受任何后续的勒索软件感染。

许多公司还额外审查了电子邮件的安全管理，努力减少潜在的欺诈邮件数量。其执行的措施，诸如在流转至内部电子邮件系统之前加强对发件人的身份验证，包括使用“发件人策略框架”（SPF）验证系统。SPF可以确认某一信息是来自发件人公司相关联的合法域名；但还有必要进一步检查以过滤出潜在的恶意内容。

评估人的行为

显然，系统可以缓解人工操作的耗时费力，但每一个人仍必须警惕风险。因此，这种风险减损技术需要考虑到人类行为中的“房中大象”态度（形容明明存在的问题却被人刻意回避）。每一个公司的结构和文化会从根本上影响其员工，以及合作方在面临网络威胁和漏洞的反应方式。明晰的公司政策（包括有关举报的内容），和有效的、定期提醒，以及良好的实践培训都是必要的减损方法，至少可以解决内部粗心所致的威胁。例如，拥有发现可疑邮件并予以正确处理的能力，仍然是至关重要的。

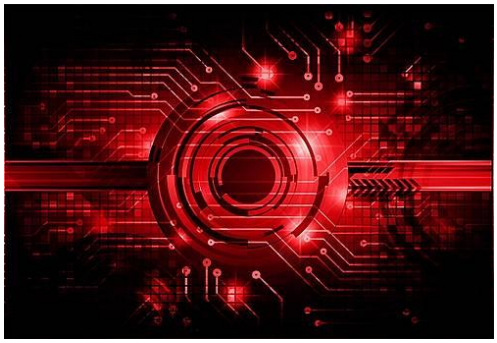
“认识到人们在工作场所之外的生活”

此外，还必须清楚地认识到人们在工作场所之外的生活。企业需要考虑到设备的接触范围，如智能手机，更不用说通过使用社交媒体所呈现出的潜在漏洞。在个人和企业层面，需要平衡考虑边界网络安全性和易使用性。这不仅包含设置复杂的密码/PIN等事宜，还要明确有关连接以及外部设备和USB闪存设备的使用事项。

“对网络风险的评估进展缓慢，并且可以发现对周边的防御措施也是不足的”

结合现实情况，信息通信技术对于实现个人和企业的目标而言，已是非常普及的技术，但对网络风险的评估进展缓慢，并且可以发现对周边的防御措施也是不足的，所以我们应重点关注人为因素以及发展侦测和修复技术。迄今为止的经验可能仅能应对一些小规模的事件。

2．网络经验教训：应两手抓



最近海事部门对有关网络风险所采取的行动，可以说向多式联运业提供了一些有用的经验教训。接下来我们鼓励去应用这些经验。

国际海事组织（IMO）海上安全委员会于2017年6月召开了第98次分会议（MSC98）。在许多重要的相关事务中，持续了有关网络安全的早期讨论，并重点关注了海运模式与重要船舶/港口的相互作用。

随着事态的发展，特别是发生了“NotPetya”网络攻击事件后，此类讨论和事后所采取的行动早已谈不上为时过早，事实上，业内许多人仍可能尚未考虑这些风险。海事IT安全专家CyberKeel最近表示，“易受网络攻击是航运业的通病，44%的承运人呈现出低水平的网络防护”。此外，SeaIntelligence的Lars Jensen透露，排名前20的某一班轮承运人允许在其电子商务平台上使用“x”作为密码，而另一班轮承运人将“12345”定义为“中等强度”的密码。

近期网络攻击事件之后，TT Talk：运输链中的电子风险一文曾向业界发出呼吁：建议重新审核应对机制，并要求执行更强大且更弹性化的流程和系统。在国际贸易中，现有趋势将推动企业数字化进程、改善内部流程，与利益相关方进行系统对接，以及调查自动化的可能性。与安全和效率有关的机遇是非常好的；但也充满了风险。

海运

所有这些进步都取决于信息和通信技术（ICT）的进一步发展，这将不可避免地增加与广大交易方和利益相关方接触的次数和复杂性。MSC 98次会议上进行的讨论已认识到这些问题，尽管讨论主要集中在与船舶的系统和网络有关的风险。本次会议有两个相关成果是非常重要的。

首先，委员会通过了关于实施网络风险管理的MSC 428（98）号决议。因此，船东和经营人将需要考虑安全管理系统中存在的此类风险，并确保网络风险不能在晚于2021年1月1日之后的第一个年度审核前解决。

其次，MSC 98批准了“海上网络风险管理指引”的文件，并与IMO促进委员会（FAL）联合发布了一份通函（MSC-FAL.1/Circ.3）。根据通函内容，这些指导意见迎合了对提高网络风险威胁和漏洞认识的迫切需要：“该指引提供了关于海事网络风险管理的高级建议，以保护航运业免受目前及新兴的网络威胁和漏洞。该指引还包括支持有效的网络风险管理所需要的功能要素。”

其他人应遵循

随后，由BIMCO牵头与一些海运业的利益相关方，发布了“船上网络安全指南”第2版。这后一种指南内容更为广泛，为可能需要考量的风险管理提供了宝贵的背景介绍和扩展意见。虽然该指南旨在协助船舶利益相关方，但TT Club建议运输链上的各利益人也用它来评估业务操作、制定适当的可维护安全的程序和行动。港口不可避免地会与船舶有至关重要的联系，所以一些国家当局可能会详细地运用这些指南，但坦率地说，我们希望它可以被更广泛的运用。

正如MSC.428（98）号决议所提到的，还有其他信息安全架构，如ISO 27001，其通过有效的技术手段为信息安全提供了整套方案，包括审计和检测、政策和流程以及员工意识。ISO 27001使用的信息安全风险管理办法，可确保企业应对最新的网络威胁和安全风险。在处理审计方面，ISO 27001还可以将这一过程进一步加固。

来自海事部门的举措肯定是值得欢迎的，尤其是因为对网络问题的评论太多了。毫无疑问的是，企业（和他们的保险人）就网络所暴露的问题证明，技术进步比起一般的准备工作，能更快且有效地吸收和缓减这些风险。这与推动变革的因素结合在一起，意味着所有的讨论都能提高防患意识、风险评估、质询水平和（适当）公开违规行为，这是值得欢迎的。

“技术进步比起一般的准备工作，能更快且有效地吸收和缓减这些风险”

对于整个运输链中所涉及的人员，特别是非海运过程中的利益方，在出席10月份举行的ICHCA第65次会议时，可以有机会对这一重要但又广泛的话题有进一步了解。

3. 法律焦点之电放问题思考

在国际贸易中寻求电子简化而涉及的风险远远超出了技术所能解决的范围；这里对现有的合同操作进行了整合评估。

事实背景

在2011年1月至2012年6月期间，由Glencore公司托运，MSC（地中海航运）负责从佛里曼特尔往安特卫普运输了69批钻块。承运人每次都用电子邮件向提交提单的Glencore公司的代理人（和提单下的到货通知人）发送放货通知书，其中含有四位数PIN码。该放货通知代替了交货单。而随后司机可使用PIN 码进入码头并提取货物。这需要有一个电子放货系统（ERS）方能操作，该系统自2005年以来，在安特卫普被一些班轮公司和代理人在“自愿”的基础上使用。

当司机代表Glencore的代理人准备提取第70批货物时，发现提单上载明的三个集装箱有两个丢失，可以推断是被未知人员入侵ERS系统偷走了货物。Glencore公司以违反合同、侵占为由起诉MSC，因为只有在提供提单，或交换提单时用的交货单才能交付货物。

承运人一审抗辩不成功，随后上诉。

引起的争论

MSC形容PIN码即是一个象征符号，并声称将其发给Glencore公司的代理人后即构成货物象征性交付。这里有一个问题，PIN码的交付与物理上交付货物并不相同——承运人可以在收货人提货之前取消PIN码（即使这样会违反合同）。然而上诉法院认为，如果双方有明确同意使用ERS系统，那么这个交付本可以成立。但在这个案件中，提单上的内容并没有此类约定。

承运人声称包含PIN码的发货通知是根据提单要求给出的交货单，并且符合英国COGSA（海上货物运输法）的要求。这一论点被法院驳回，因为放货通知缺乏交货单的本质特征——即根据COGSA的规定，明确或默示承诺按照提单条款向收货人交付货物。

承运人提出的其他论点，包括提单条款已经由交易习惯或过往的沟通而改变，或由于Glencore公司的代理人通过ERS系统接收了前69批货物，所以Glencore公司的行为构成禁止反言等，也未成立。根据事实这些论点被一一驳回，因为这些论点与提单条款不一致（或明确冲突），而且Glencore公司或其代理人未曾明确同意接受使用ERS系统。Glencore公司并不知道ERS系统的存在，且其代理人只是容忍MSC自愿决定使用该系统。这个案件抛出了一个技术方面的问题，即在代理关系中区别衡平法的禁止反言和放弃合同权利的不同。

结论

虽然此案是基于事实所做的判决，但可以从中吸取经验教训。如果希望通过电子系统代替纸张来简化交货过程，则必须注意确保双方之间的合同内容明确这一点，并在提单或其他运输合同中可以得到证明。

地中海航运公司 诉 嘉能可斯特拉塔股份有限公司（‘MSC Eugenia’）
[2017] EWCA Civ 365

结束语

我们真诚地希望上述内容对您的风险管理有所帮助。如果您想了解更多信息，或有任何意见，请给我们发电子邮件。我们期待着您的回音。

百富勤·斯托斯-福克斯(Peregrine Storrs-Fox)
风险管理总监
TT Club

TT Talk是TT Club不定期出版的免费电子通讯文件，原稿由TT Club伦敦发放，其地址是英国伦敦芬彻奇街90号，邮编EC3M 4ST。(90 Fenchurch Street, London, EC3M 4ST, United Kingdom)

您也可以登录我们的网站阅读本通讯和过去所有的通讯文件，网址是：
http://ttclubnews.com/2RU-53ETA-0DGCHMVA76/cr.aspx

者、文章材料的撰写者及其他相关工作人员，以及 TT Club 协会本身，对于任何依赖 TT Talk 信息内容所造成的灭失与损害将不承担法律责任。

如果您想要了解本公司的登记注册信息，请点击以下网址：
http://www.thomasmiller.com/terms-and-conditions/company-information/