July 2021. Issue 276 in the series

TT Talk 第276期

1. 采购欺诈
2. 供应链中的网络犯罪：更有针对性、更复杂
3. 法律焦点——想要赔偿更多

1. 采购欺诈

在日常的业务工作中，每个公司都会产生许多交易，以支持其经营活动。无论是物流服务、重要的供给（如燃料）或简单的日常补给，采购工作不仅频繁且现在几乎完全靠电子化交易完成，这增加了采购过程中的欺诈风险。

继续我们的提高防欺诈意识专题，本篇我们将叙述采购欺诈，了解它对全球物流供应链企业的影响，尤其是当今快节奏的数字化环境更有利于这一诈骗的发展。

要降低风险，有效的尽职调查至关重要。无论采购的价值或频率如何，也不管您的供应商是在同一工业区还是另一个大陆，关于尽职调查的基本原则都是一样的：任何时候都清楚地知道您在和谁交易。

“任何时候都清楚地知道您在和谁交易”

常见的采购欺诈方案有很多种。这里我们关注两种：一是重复或假发票、二是虚假的供应商。

重复或假发票

什么是重复或假发票？

这种发票欺诈行为包括故意提交假的、重复或虚报的发票，并声称来自已知的供应商或承包商。实际上这是由一个欺诈人提交的，他通过渗透您的业务流程，来欺骗您的企业支付不应支付的金额。

无一例外的是，任何付出的款项都会受到欺诈人的控制。错误的交易一段时间后才能被发现，而在此之前资金已经被转移，通常经一系列的其他银行转移后，资金将永远消失。

这种类型的欺诈具有一定程度的复杂性，它能剖析出您企业交易的类型、与谁、以何种频率以及以何种近似价值做交易。我们发现，对受害者进行剖析、渗透入电子邮件系统、以及篡改电子文件所需要的成本投入或专业技能门槛相对较低。开具一张看起来真实又不会触发额外审查的发票从没有像现在这样容易。

“开具一张看起来真实的发票从没有像现在这样容易”

实施这类欺诈的人通常会使用容易混淆的电子邮件地址，并将目标对准他们一直在监视的个人，使他们面临立即付款的压力。欺诈人可以用几乎相同的电子邮件地址和熟悉的语言语调，把自己伪装成一个已知的联系人。他们可能会声称发票已经过期，或声称对企业信用评级或商业信誉产生负面影响，并威胁在不付款的情况下采取法律行动，以迫使交易通过。

这是怎么发生的——举一个真实的例子

X物流公司从Y油品公司采购所有的卡车燃料。某天，由于季节性假期，当值员工不多，一个自称来自Y油品公司的人联系到了在X物流公司会计部门工作的John。Y油品公司的代表很生气，要求立即完成一笔未偿付的款项。John 收到了一张似乎挺合理的发票，但在会计系统中却没有记录。Y油品公司的代表威胁要严格限制其可用的支付信贷安排，John认识到这对公司将是一个灾难性的局面。他不愿意承担这一风险，随之安排付款。第二天，John打电话给Y油品公司，为自己的疏忽道歉，并要求他们确认收到了这笔款项。但Y油品公司没有人知道前一天的发票和电话的事情。诈骗人截获了一份较早的发票，伪造了一份副本，并说服X物流公司进行付款。

虚假的供应商

什么是虚假供应商？

虚假的供应商采购欺诈是一种内在威胁，涉及对关键信息和系统有访问权限、并拥有足够的操作知识来掩盖其行为的人员。

“涉及对关键信息和系统有访问权限、并拥有足够的操作知识来掩盖其行为的人员”

欺诈人（通常是一名雇员），会在账户系统中创建一个虚构的供应商。所有“了解您的客户（KYC检查）”和尽职调查程序可能都会通过。随后，虚构的供应商提交发票，这些发票都会被正式审核和会被支付，就像真的一样。

这类欺诈可能很难被发现，它取决于您业务的规模和结构。

这是怎么发生的——举一个真实的例子

John在P物流公司的会计与合规部门工作，他创建了一个名为Q油品公司的新供应商账户，并完成了所有必须的KYC验证要求。附在Q油品公司账户上的银行信息是John控制下的银行账户。每隔一个月，John就会开具一张价值约2,000美元的虚假发票，为了避免怀疑，他没有使用四舍五入的数值。每次John都将发票录入账户系统，并正式授权付款。

减少采购欺诈的风险

在业务繁忙的时候，想要发现某一虚构的公司或业务将会非常困难，特别是在企业人员不足或远程办公的情况下。诈骗人通常会研究受害人，以便在一个最薄弱的时机出手。

应开发和测试管理控制流程，其中应包含健全的尽职调查、“四眼”检查和升级程序。提高防欺诈意识的培训将增加您在业务中发现诈骗的可能性，而升级程序将加快调查，使那些有权力保护企业的人做出决定。

TT Club关于避免采购欺诈的小贴士：

- 定期讨论与欺诈有关的内容，有置疑的能力并保持适度的追究心态
- 警惕内在威胁，并制定有效的举报程序
- 并入一个含多步骤、独立的付款授权流程；不要着急，先“休息五分钟”
- 对现有账户信息的任何更改，应制定严格的验证流程（如：打电话给一位已知的联系人以验证请求）
- 仔细检查您银行的对账单，并向您的银行报告任何可疑的活动
- 最重要的是，要认真对待这一点：即使是最有经验的员工也有可能被骗。

“最重要的是，要认真对待这一点：即使是最有经验的员工也有可能被骗”

2．供应链中的网络犯罪：更有针对性、更复杂

全球约有90%的贸易是通过海上运输完成的，加上新冠肺炎疫情带来的物流困境和网络犯罪的新动向，可以说供应链中的网络安全变得前所未有的重要。

物流供应链不可避免地成为黑客眼中极具吸引力的目标，因为它涉及到多个司法管辖区的众多参与人，都使用常见的应用软件。一旦某个公司的软件遭到侵入，就有可能在全球范围内暴露出一系列企业的漏洞。

“物流供应链不可避免地成为黑客眼中极具吸引力的目标，因为它涉及到多个司法管辖区的众多参与人，都使用常见的应用软件”

近年来，我们对整个海运供应链脆弱性的认识不断加强。国际海事组织（IMO）也意识到了这一点，并在现有的《国际安全管理（ISM）规则》的框架内强制实施网络风险管理。然而，仅针对海运网络安全的必要关注不应被视为万能灵药。TT Club与UK P&I Club合作，在2018年就强调了船舶/港口货物交接的风险；在这一期间，网络犯罪的活动只会增加。

仅去年一年，就出现了多个漏洞，每个漏洞都可能被网络犯罪所利用。新冠疫苗的运输威胁正在风口浪尖之上，与此同时苏伊士运河阻塞的影响也仍在继续，且持续不断的疫情风险也在产生麻烦，例如最近盐田港的疫情。

什么是供应链网络风险？

网络风险可以定义为由于电子系统故障和网络技术故障而造成的货物灭失、损坏或营业中断的风险。在实践中，就是我们谈论的黑客非法入侵信息技术（IT）或操作系统（OT），有可能使控制失效、扰乱经营活动、或释放、修改或毁坏数据。

在海事领域，这种网络攻击可能包括射频（RF）技术，这意味着全球导航卫星系统（GNSS）和自动识别系统（AIS）干扰和欺骗都是可行的攻击方式。这对航行和安全通行都有重大影响。

同样，在港口基础设施中使用的码头操作系统，例如货物装卸设备，也同样容易受到潜在的破坏。疫情导致的混乱和远程工作所暴露出的问题只会加剧欺诈的风险。

最新的威胁包括：

- 网络犯罪的手段**越来越高明**。勒索软件攻击比以前更有针对性，网络犯罪不再采取“霰弹枪”式的方法，而是对目标进行评估。可供网络犯罪所使用的工具正越来越多。
- **更有针对性的攻击**，根据目标的情况量身定制方案。过去，可能就是一个简单的手段，索要500美元价值的比特币来重建系统访问权限。而如今，所使用的手段与公司的营业额规模挂钩。根据对目标公司实施拒绝服务等攻击所造成的可能价值损失、营业额和现金储备等影响，来制定具体的勒索金钱数额。
- **改变方向**。之前勒索软件的攻击只涉及简单的拒绝服务，现在攻击者可能不仅会通过让人无法访问系统来增加威胁，还会在暗网上发布或出售敏感数据。
- 承包管理网络安全的**第三方服务供应商**本身也成为了网络犯罪分子的目标。人工智能应用安全公司ImmuniWeb最近的一份报告显示，2020年有97%的主要网络安全公司的数据被暴露在暗网上。

除了经济利益的明显动机外，还有一些记录表明，利用全球供应链的固有属性（即能促进跨国贸易的系统和程序）来进行非法贸易，主要发生在麻醉类毒品和人口贩卖上。

减轻网络风险

TT Club定期会强调严谨的网络风险管理的重要性，并敦促董事会和管理层进行全面评估，包括分析关键安全数据的完整性。“前十种”措施可能是这样的：

1. 加强“电子防火墙”，确保只有经过批准的软件程序才能在系统和网络上运行
2. 确保所运用的软件补丁更新勤且运行快
3. 确保杀毒软件有效，且有强大的垃圾邮件过滤功能
4. 将IT和OT的系统设计分隔，目的使受病毒影响的区域可被隔离和检查
5. 定期对关键数据进行备份，包括确保备份文件处于离线状态
6. 教育员工不要下载怀有恶意的内容，不要打开不安全的网络浏览器，不要成为社交攻击和钓鱼诈骗的受害者；训练员工能识别并报告网络威胁
7. 通过行业内和跨行业的合作，来提高相关意识并识别网络威胁的趋势（包括开放更多的共享信息）
8. 制定一个强健的事故响应计划，有一个准备充分和目标明确的专有团队
9. 制定强健的应急计划，因为充分的准备是攻击期间或攻击之后恢复的关键
10. 保持警惕，做好被攻击的准备；不是会不会发生的问题，而是什么时候会发生

“保持警惕，做好被攻击的准备；不是会不会发生的问题，而是什么时候会发生”

总结评论

近几个月来，无论是通过媒体屏幕，还是通过商场里空空如也的货架，世界上大多数国家的民众对全球供应链的风险意识都得到了加强。许多人也会知道最近有勒索软件攻击美国燃料供应商——Colonial Pipeline，它有效地关闭了他们的供应系统。

在全球供应链中，大家的警惕意识受各国经济发展的影响，会有所不同。随着更具有破坏性网络活动的增加（无论是由犯罪分子发起，还是更险恶的国家行为），所有利益相关人都必须为不可避免的情况做好准备，建立能抵御不断演变的网络威胁的能力。

现实是，所有的企业都容易受到像“Colonial Pipeline”事件的影响，这很可能是由于员工没有发现钓鱼邮件，并启动恶意链接造成的。

进一步的见解可参考：

《风险聚焦：考虑海运供应链中的威胁》
《港口企业网络安全白皮书》

3. 法律焦点——想要赔得更多

一个有趣的案例表明，在没有采用或实施近期通过的议定书、甚至是国际公约的地区，不同的司法管辖区可能存在赔偿限额差异，这与国际保赔集团（International Group of P&I Clubs）最近要求提高赔偿结果的确定性和一致性的呼声相呼应。

事实

“Milano Bridge”轮撞上了釜山港的桥吊，随后韩国政府和码头营运人要求赔偿维修和业务中断费用。船东要求适用韩国的责任限制。

根据韩国法律，船舶的责任限额是由船舶的船旗国决定的。在本案中，该船船旗国是巴拿马。后者批准加入了最初的《1976年海事赔偿责任限制公约》（LLMC），大约需要赔偿的数字是2400万美元。

码头经营人在韩国和日本同时提起了民事诉讼，后者是该船的管理人所在地。随后，码头方在香港扣押了一艘“Milano Bridge”轮的姐妹船，并取得了金额为8300万美元的担保函。该数字是根据香港法律计算的，香港通过了1996年的议定书和2015年的LLMC修订版（类似的责任限制也适用于日本法。）

该船东以不便管辖原则为由，向原诉讼法庭申请中止香港的诉讼程序。

判决

香港法院采用了1986年英国上议院“Spiliada Maritime Corp 诉 Cansulex”一案中提出的两个验证步骤，并得到了香港终审法院的认可。第一步是由被告来承担举证义务，来证明原告提起诉讼申请的法院“不是自然的或适当的法院”，以及证明另有一个更适当的管辖地法院供选择。如果这一条件得到满足，法院通常会批准中止诉

讼程序申请，除非原告能证明为什么不能这么做。第二步要求原告证明，如果诉讼程序中止得以通过，他将遭受司法或个人的不利对待。

法院根据香港的判例发现，如果诉讼程序没有被中止，基本上就会产生责任限额的差异。某一个判例的情况，比较自然的法院选择应该是印度尼西亚，但其责任限额是不确定的，且少得可怜。而另一个判例的情况是，有一个自然法院，但双方都没有选择它。还有第三种情况，被告是一家香港公司，所以没有能通过Spiliada测试的第一步。

在本案中，大家都认同香港不是自然或适当的司法管辖地。然而，原告韩国方声称韩国也不是更合适的法院。原告进一步主张说，如果因为被迫在韩国进行诉讼而获得较低的责任限制赔偿数额，等于剥夺了他的司法权益，而这一点才是决定性原因。

法庭认为，韩国显然是更合适的管辖地。该事件发生在韩国，目击证人也在那里，许多相关的文件是韩文的，该事故所适用的法律也是韩国法。

法院驳回了原告的观点，即司法利益的问题是决定性的，并认为事件在与香港的联系等其他方面都很薄弱的情况下，仅仅取决于扣船的地点，法院仍有理由拒绝中止程序。而原被告双方均没有任何相关人员常驻香港的事实，进一步削弱了其论点。

法院对于纯粹因为经济因素而选择管辖地法院的行为不太同情，并表示作为一家韩国公司，原告应接受其经营所在地的司法管辖原则。法院还推测，原告过去可能从韩国较低的责任限额中受益，以及由此带来的保险费用也较低。

评论

如果这一申请成功，其实际效果将是：在香港扣船，只因为香港有更高的责任限额，而不管其他因素，就赋予原告在香港的司法管辖权。这将是一个令人惊讶且不受欢迎的结果。如果事实不是那么清楚，例如如果是在公海上发生碰撞，那么结果可能会有所不同。

原告已申请上诉。

这虽然是一个香港的案件，但其判决一定程度上参考了英国上议院的判例。此外，它清楚地向全世界表明，香港在司法管辖权方面不是一个容易妥协的地方。

PUSAN NEWPORT CO LTD 诉 OWNERS OF MILANO BRIDGE & CMACGM MUSCA+HYDRA
[2021] HKCFI 1283

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：
https://ttclubnews.com/2RU-7G1PP-14A77BE39122EB78WBHHIN5CAD606EC3BBEA7C/cr.aspx

我们在此声明，TT Talk 中的全部内容仅供参考，不能代替专业的法律意见。我们已采取谨慎措施，尽量确保此份电子通讯的材料内容的精确性与完整性。但是，编者、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/