KPMG
毕马威

2024网络安全重要趋势：能源及天然资源行业

转型赋能

能源行业包括电力和公用事业、油气、天然资源和化工等子行业。这些子行业的运营模式以及与客户和供应商互动的方式正在经历重大转变。在能源密集型行业（如制造、科技和汽车）中，企业也在同步转型，进一步加剧了能源行业面临的复杂形势。

能源已经融入当今社会生活的方方面面。为适应不断变化的世界格局，能源行业正在重构其价值链，努力打破能源行业只局限于加油和供电的刻板印象。

能源行业当下的重心是通过可再生能源和清洁能源，尤其是二者的整合以及数字化来推动能源转型。

这种转型不单影响着能源行业。事实上，从信息技术和运营技术的角度来看，全球经济的各行各业都因此经历着巨大转变。

无论是石油钻机上的阀门还是发电厂的计量设备，它们所连接的控制网络和系统均处于“永久运行”的状态，从而产生了永久的安全风险，并重新定义了整个能源行业的攻击面。

本文探讨了对能源及天然资源行业至关重要的网络安全考虑因素和主要措施，概述了网络威胁不断演变的格局，并提供了深刻洞察，旨在帮助能源企业网络安全和业务负责人员在未来一年里高效履职。

考虑事项1：应对不断模糊的全球边界

能源及天然资源企业可能需要继续通过扩大全球客户群和全球足迹来拓展业务，而不受其所在司法辖区和总部位置的限制。行业网络安全专业人士所面临的最大问题是在业务赋能和业务价值之间取得适当平衡，同时确保满足监管机构的预期。这种平衡非常微妙，同时颇具挑战。

主要挑战

司法管辖区的复杂性

在多数情况下，不同国家、地区和司法管辖区制定了不同的网络安全监管框架。某些法规更注重方法的统一性，例如《网络与信息安全指令》（NIS2）尝试在欧盟推广一致的实务方法，而其他某些地区则更强调因地制宜，导致对法规的诠释存在差异。因此，能源行业的监管合规形势愈加复杂。能源企业既要遵守全球或地区标准，又要满足当地规定。

电网稳定性和新增攻击面

随着能源行业的全球互联水平不断提升，相关网络威胁的攻击面也在不断增加。各种系统和网络的跨国整合为网络犯罪分子提供了更多切入点，对互联跨境能源网络的电网稳定性造成了威胁。

网络跨越边界

网络威胁不受地缘政治边界的限制。一个国家遭受的网络攻击很容易影响另一个国家的关键基础设施。在这种情况下，通常难以协调应对措施并对网络攻击进行归因。

信息共享的法律限制

尽管协作和信息共享能有效确保网络安全，但跨国界共享敏感信息所涉及的监管、法律、政治和竞争问题，可能会阻碍威胁情报共享。

持续的商业政治化

能源及天然资源行业中的商业/经济活动容易受政治利益、议程和效应的影响。地缘政治局势紧张往往会导致网络威胁增加，尤其是针对关键基础设施的网络威胁。作为一个关键基础设施行业，能源行业是网络破坏分子和国家支持的行为者的主要攻击目标，对供应链和终端消费者均可能产生影响。

主要机遇

协作

能源行业的全球化性质为网络安全的国际协作提供了契机。在全球范围分享威胁情报、行业最佳实践和经验教训可以增强能源企业的整体安全态势。

标准化

全球化可以推动能源行业建立网络安全的国际标准和最佳实践。此外，规范的规章制度可以简化网络安全措施的跨供应链和跨边界实施。

创新

跨境合作可以促进开发先进网络安全解决方案，从而惠及整个能源行业。

灵活性

通过全球通信网络，事件响应团队可进行实时合作，从而快速就网络威胁作出更有效的应对措施，最大程度降低网络攻击对关键基础设施的不良影响。

能源及天然资源跨国企业在跨境经营过程中面临各种挑战，例如全球化速度加剧的商业环境、高度复杂的监管制度和不断演变的攻击面。面对上述挑战，许多小企业准备不充分，但它们可以借鉴大企业的成熟做法，以免作无谓的努力。

考虑事项2：供应链安全现代化

第三方环境中存在的威胁处于不断演变的状态。这种威胁可能存在于各项新技术和流程之中，还包括供应商可能未严格遵守企业安全协议的情形。为此，基于供应商的成熟程度，能源企业可能需要视情形进行月度审查，或每季度进行一次审查（赋予供应商更多自主权），以确保与第三方的关系高效合规。尽管存在诸多挑战和亟待解决的优先事项，但为确保供应链生态系统安全而作出的努力不应成为阻碍业务发展的瓶颈，而应成为推动业务发展的动力。

主要挑战

供应链的复杂性和依赖性

能源及天然资源行业的全球化性质增强了其对复杂供应链的依赖性。在能源行业这个由多层次利益相关方、供应商和技术提供商组成的生态系统中，想要清楚了解和控制各方近乎奢望，从而极大地增加了网络风险。

新技术 VS 旧技术

能源企业通常依赖新旧交融的信息技术（IT）和运营技术（OT）。互联网技术的采用加剧了这一复杂性，随之而来的是更多的相互依赖关系和潜在漏洞。运营技术系统通常比信息技术系统具有更长的使用寿命和生命周期，并且相对于新技术而言，旧技术的安全性往往更低。对于企业而言，整合各种技术体系（即新旧技术体系）和相应的安全措施，虽然是底线，但极具挑战，并会因数字化的加剧而愈加难以实现。

最薄弱环节

在整个供应链中，运营商和供应商在网络安全成熟度方面的差异，可能会对整个供应链产生级联影响，从而形成薄弱环节。为此企业需要依赖第三方尽职调查 — 网络安全性较低的供应链合作伙伴也会影响企业的安全态势。在生态系统中跟踪所有供应商和合作伙伴的网络安全态势及措施可能十分困难。

数字化

在不断发展的能源市场中，向绿色能源转型和客户需求的不断演变均要求企业拥抱数字化和创新。与此同时，新技术的采用也引发了人们对所涉网络安全问题的关注。

主要机遇

透明度和协作

在管理与第三方供应商相关的网络安全风险（包括评估其安全实践）方面，能源企业可能面临挑战。但在这种相互依赖关系的推动下，企业迫切需要提升供应商的网络安全透明度和协作水平。提升安全态势和措施、数据泄露和漏洞的透明度，有利于营造一种文化氛围，鼓励相关人员积极识别薄弱环节，并提出集体解决方案，从而使消除供应链薄弱环节成为可能。

信息共享

能源行业利益相关方的合作形式还可以包括共享威胁情报和最佳实践。这将有利于改进集体的网络威胁防御措施。

可见性和创新

在供应链中引入新技术可以提高运营效率，并提高企业的可见性和监控能力。据此，企业可以降低网络安全风险，并提高事件识别和恢复能力，从而强化供应链的安全性。

目前，许多能源企业正处于网络风险管理的早期阶段，触达了供应链的第二层级，但多数情况下，这一管理流程并未深入至第三和第四层级。随着法规（如欧盟的NIS2指令）不断演变，企业及其第三方供应商可能被要求采取适当措施来管理网络安全风险，以预防或最大程度地降低网络安全事件的影响。

考虑事项3：网络安全与企业韧性相结合

能源及天然资源企业需要不断提升韧性。韧性意味着准备充分，能够快速、全面地处理事件，并将业务影响降至最低（至少是可控水平）。随着网络安全环境的持续变化，企业不应将韧性构建视为一系列孤立的或间歇性的计划组合，而应视其为一项适应性战略。这项战略旨在补充和强化企业的网络安全议程，不仅保护客户利益免受侵害，还要确保与企业的整体业务目标紧密契合，同时专注于创造和实现长期价值。

主要挑战

运营韧性

能源企业深谙在交付关键服务时保持高水平的运营和韧性的重要性，任何中断都可能产生重大影响。企业必须深刻认识到，网络攻击的目标不仅是企业的信息技术基础设施，还包括企业整体业务运营及其所处的行业环境。为保持网络韧性，企业需要转变思维，积极培养新能力并制定新的安全措施。

行业环境的复杂性

能源、电力、储能和可再生能源等基础设施行业的环境最为复杂，并对社会和经济活动发展起着举足轻重的作用。未能充分了解所有系统的功能、互连性和依赖性可能会阻碍企业在构筑韧性方面的进展。

供应链韧性

能源及天然资源企业对第三方、第四方甚至第五方供应链合作伙伴的严重依赖，使得提升事件恢复力和总体韧性尤其困难。

威胁态势

威胁态势的愈演愈烈要求能源企业不断评估和更新其防御和应对计划，以有效应对不断演变升级的威胁。

信任和声誉

保持客户的信任是能源行业安全专业人士的重要职责。网络安全事件不仅会导致企业运营中断，还会削弱客户对企业的信心。为了管理网络安全事件对客户信任和企业声誉的影响，企业需要采取积极、透明的网络安全策略。

主要机遇

前景

为保持韧性，企业需要更为全面地理解和管理风险，其中不仅涉及网络安全威胁，还包括可能干扰运营的其他各种因素。这种全面的方法有助于企业转变思维，并识别更广泛的风险。

适应能力

对威胁态势演变、技术进步和商业环境变化的适应和响应能力是企业具备韧性的标志。据此，能源企业能够在新挑战出现之前迅速调整和启用新的网络安全和运营策略和能力，例如采取更加完善的检测和监控措施。

协作

落实韧性举措，通常需要与其他行业的合作伙伴进行协作。建立强有力的伙伴关系，并跨行业共享信息，可增强集体的防御和应对能力。

合规

采用以韧性为中心的方法，有助于企业在确保遵守网络安全法规的同时，满足与业务连续性、灾难恢复和综合风险管理相关的更广泛的合规要求。

在全球持续动荡的情况下，关键基础设施仍将是网络攻击的重点目标。能源行业在确保运营韧性方面可借鉴以往经验，但领导层必须转变思维，重点关注包括网络安全在内的整体韧性。

能源行业的网络安全现状

总体而言，能源行业因其重要性以及与其他行业的关联性，一直是网络犯罪分子频繁攻击的目标。

例如，最近一次油气管道袭击事件对多个行业造成严重干扰，导致供应短缺、价格上涨和供应链中断等问题。该袭击事件还导致依赖油气基础设施的其他行业（如航空业）发生停运和服务中断，因为油气管道是航空燃料的主要来源之一。

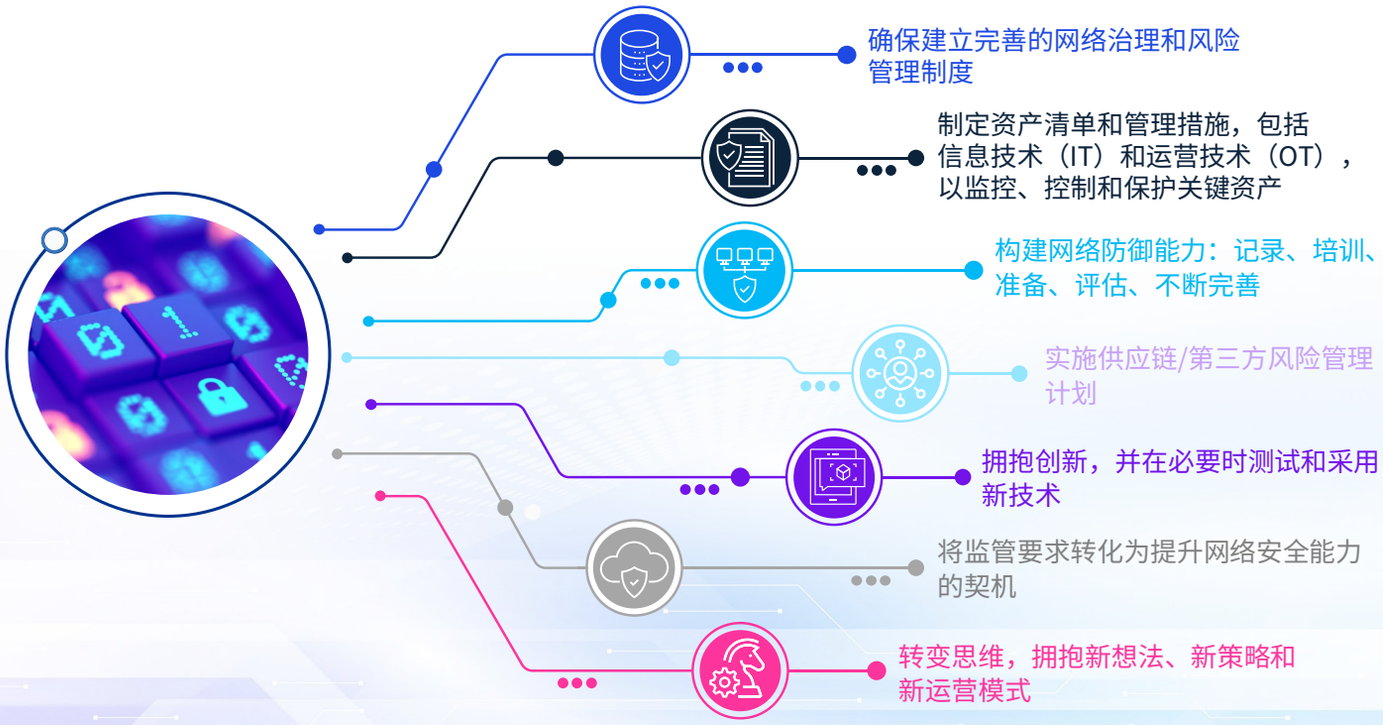
这一事件暴露了关键基础设施的弱点，并引发了公众对能源行业总体韧性的担忧。因此，许多能源企业面临着增加网络安全投资，加强漏洞评估和渗透测试的压力，以识别薄弱环节并修复任何安全漏洞。

许多关键基础设施企业还设立或强化了安全运营中心（SOC）和网络安全事件响应小组（CIRT），以监测和应对潜在的安全事件，最大限度地减少损失并迅速恢复运营。

我们建议能源及天然资源企业将技术、培训、应对能力、信息共享和恢复计划相结合，从多个层次来管理网络安全。

另一值得注意的考虑事项是，人工智能的兴起比预期的更为迅猛。人工智能对能源及天然资源行业而言是一把双刃剑，我们将在另一篇文章中对此进行深入探讨。

网络安全专业人士的首要任务



毕马威可提供的协助

毕马威专业人士可协助企业评估网络安全计划，并确保计划与企业的业务优先事项保持一致。此外，我们还可以协助能源及天然资源企业开发先进的数字解决方案，针对方案实施和风险监控提出建议，并协助企业设计应对网络事件的适当措施。

毕马威专业人士擅长应用领先思维来分析能源行业最为紧迫的网络安全问题，并为企业提供量身定制的解决方案。毕马威专业人士凭借安全可靠的技术为企业提供了大量解决方案，包括网络云评估、隐私自动化、第三方安全优化、人工智能安全以及受客户委托管理风险检测和响应工作。

想了解更多毕马威可提供的转型服务，请联系我们。

蔡忠铨
毕马威中国董事
能源及天然资源行业主管合伙人
毕马威亚太区及中国
alex.choi@kpmg.com

张令琪
网络安全和数据保护服务
主管合伙人
毕马威中国
richard.zhang@kpmg.com

张龙华
科技赋能服务主管合伙人
能源及天然资源行业
毕马威中国
longhua.zhang@kpmg.com

黄芃芃
网络安全和数据保护服务
合伙人
毕马威中国
quin.huang@kpmg.com

kpmg.com/cn/socialmedia