KPMG
毕马威

2025能源行业网络安全重要趋势

能源行业首席信息安全官
肩负着前所未有的信息技术
安全职责

kpmg.com/cn

对于全球能源企业而言，其网络安全状况正因一系列影响因素而悄然发生变化。这些因素包括首席信息安全官职责的扩大、人工智能和物联网等信息技术的广泛应用，以及建立具有韧性的企业文化和网络环境的迫切需求。在当前复杂且相互关联的环境下，该行业许多首席信息安全官正着力提升员工的数字意识，以应对面临的前所未有的挑战和机遇。为此，他们必须承担起网络安全倡导者的角色，在组织的各个层面激励和鼓舞员工将认知付诸行动。

在能源行业中，首席信息安全官的职责不再局限于传统的信息技术安全范围。事实上，毕马威的调查显示，该行业70%的受访首席执行官认为，网络犯罪和网络安全问题将在未来三年影响企业发展。[1] 随着信息技术和运营技术的融合，首席信息安全官如今肩负着保护从管理到生产的整个技术生态系统的职责。

履行新的职责需要具备新的技能。首席信息安全官必须有效地让高级管理层认识到网络安全对企业的影响，确保获得足够的预算，并在内部打造具有韧性的企业文化。我们看到许多积极迹象表明，企业在如何进一步将网络安全融入自身组织方面取得了进展。我们的调查发现，在能源行业中，59%的受访者表示他们通常在技术投资决策初期就已将网络安全纳入考虑范围并予以高度重视。[2]

该行业特有的挑战增加了首席信息安全官工作的复杂性。能源行业在技术、网络安全和环境方面面临着若干复杂的监管要求，例如，欧盟《网络安全措施的指令》（ NIS2指令）、 北美电力可靠性公司关键基础设施保护标准和欧盟人工智能法案等。首席信息安全官在确保合规的同时，还要处理地缘政治问题和日益增多的网络攻击，这些问题都可能对企业的自身运营、利益相关方乃至更广泛的社会造成严重影响。

2024年4月，北美电力可靠性公司指出，美国电网风险点数量正以每天约60个的速度增加。[3] 在欧洲，丹麦的关键基础设施在2023年5月遭受了有史以来最严重的网络攻击，几天之内多达22家公司遭到入侵，部分企业被迫完全断开与外界的网络连接，转而采用离线运行模式。[4]

要在这种环境中实现繁荣发展，首席信息安全官必须采取积极主动的战略性思维。应提早从业务层面开展漏洞管理，并根据风险对企业的潜在影响提供战略指引；通过基于风险的方法引领实施。除战略引领外，首席信息安全官的重要职责还包括打破信息技术和运营技术团队之间的传统壁垒，确保双方团队紧密合作，共同构建持久的韧性。

在本报告中，我们探讨了能源行业在网络安全方面的重要趋势，并提供了许多真知灼见和务实建议，涵盖我们认为业内首席信息安全官在当前环境中应优先考虑的诸多领域。

[1] 《毕马威2024年全球首席执行官展望》
[2] 《毕马威2024年全球技术报告》
[3] 《KnowBe4报告指出， 关键基础设施的网络攻击风险激增30%》，Industrial Cyber，2024年8月28日
[4] 《针对丹麦关键基础设施的攻击》，SektorCERT，2023年11月

首席信息安全官应考虑的关键网络安全因素

1 首席信息安全官角色不断演变

2 智慧生态系统安全保障

3 韧性设计：为企业与社会提供网络安全保障

1 首席信息安全官角色不断演变

监管审查的加强和网络安全的战略重要性使首席信息安全官肩负着更大的责任。在某些情况下，他们还会面临个人法律责任的风险。如今，企业比以往任何时候都更加期望在网络安全保障方面能够取得成效。与此同时，传统的首席信息安全官职能也变得日益分散，许多安全和隐私职责已交由其他业务领导者负责，例如，首席安全官负责物理安全和欺诈管理，信息技术基础设施主管负责边界安全和身份及访问管理，首席数据官负责隐私管理等。

因此，首席信息安全官的职责发生了巨大转变。他们必须明确自身职责范围，与其他业务领导者密切合作，并倡导职责共担文化，以适应这一新的现实。这需要企业领导层对持续进行网络安全投资给予大力支持。毕马威的调查发现，在能源行业中，72%的受访企业的首席执行官表示，他们已经为此增加网络安全投资，以保护业务和知识产权。[5]

最终，首席信息安全官应从单一的网络安全守护者角色转变为负责打造稳健、灵活安全框架的架构师。

主要挑战

构建新的网络安全秩序

在能源行业中，首席信息安全官不仅需应对快速发展的技术，还需面对新的、具有特殊挑战性的现实问题，例如气候危机以及随之而来的增强可持续发展和环境、社会和治理（ESG）价值的压力。此外，地缘政治紧张局势，如中东和乌克兰的持续冲突，也对供应链造成了严重影响，从而增加了监管负担。事实上，毕马威的研究表明，供应链风险是首席执行官们共同面临的最大威胁，[6] 而“电力、经济中心和贸易的结构性变化，以及供应链、资产和基础设施的多重威胁”，正在对能源企业产生重大影响。[7]

因此，企业需要更多具备丰富经验和全面技能的资深安全专家，而不仅仅是技术人员，来应对这种充满不确定性的风险环境。

将网络风险界定为业务风险

首席信息安全官必须将网络风险界定为业务风险，以促进领导层和技术团队之间形成共识。战略思维、谈判技巧和卓越领导力是实现这一目标的关键因素。面对特定的行业挑战，如在保障运营连续性的同时保护数据和信息安全，获得董事会的信任至关重要。若网络安全措施（如定期安装补丁和部署适当控制）能够得到良好规划和有效实施，通常会对运营连续性产生积极影响。通过平衡网络安全的投入和价值产出，可以帮助董事会认识到相关投入对于增强安全性并缓解业务风险的重要性。

[5] 《毕马威2024年全球首席执行官展望》
[6] 《毕马威2024年全球首席执行官展望》
[7] 《毕马威2025年最大地缘政治风险》，2025年3月31日

主要挑战

监管挑战

首席信息安全官面临监管机构对企业网络安全计划有效性和韧性的严格审查。尽管在个人法律责任方面各不相同，但随着越来越多相关法规的出台，例如，美国证券交易委员会于2023年末生效的《网络安全风险管理、战略、治理和事件披露法规》，董事会在网络安全方面面临着越来越大的上层压力。[8]

融合环境中的职责划分

信息技术与运营技术的融合模糊了相关传统职务的界限，这就要求首席信息安全官同时具备技术和战略专长。明确区分业务运营和网络安全，对于避免薄弱环节及确保数字化战略的安全性至关重要。

主要机遇

- **将网络安全纳入董事会议程**——首席信息安全官可以定位为拥有关键董事会参与权和业务目标话语权的战略合作伙伴。由于首席信息安全官通常不属于董事会成员，因此建立与领导层明确且直接的汇报关系，使其能够与董事会定期沟通。
- **打破团队隔阂**——网络安全和运营团队之间的合作可使首席信息安全官发挥主导作用。将物理安全、合规、隐私和运营等领域串联起来，有助于打造全面的风险管理措施。此举能弥补技术和运营之间的差距，为实现业务目标提供支持并增强韧性。

  能源行业的首席信息安全官必须在满足可持续转型的迫切要求与保护关键基础设施的需求之间取得平衡。在持续探索人工智能驱动的预测性维护、先进储能和智能电网等解决方案的过程中，这一点尤为重要。可逐步将此类技术与现有系统进行集成，以确保短期和长期的运营连续性。

  随着基于认知的应用程序的广泛使用，首席信息安全官必须仔细权衡创新的好处与潜在的安全风险。通过数据评估，并将新兴技术的应用与业务目标挂钩，使用基于数据的见解来衡量风险并证明投资的合理性。此举有助于赢得利益相关方的认可，并确保网络安全计划具有可持续性。

[8]《网络安全风险管理、战略、治理和事件披露：小型实体合规指南》，美国证券交易委员会，2023年7月26日

2 智慧生态系统安全保障

智能设备和物联网的快速普及已使现代电网转变为一个包含众多传感器和软件的庞大互连网络，这就要求能源行业的首席信息安全官在处理数字设备安全问题方面采取根本性转变。例如，智能传感器、仪表和电网通常仅有有限的安全功能，可能会成为入侵传统运营技术系统的突破口，从而大大扩展潜在的攻击面。

此类设备所需的安全保障措施与十年前的措施存在很大不同。如今，首席信息安全官必须考虑此类智能产品的整个生命周期，从设计和开发到部署和维护。安全策略应考虑到这些设备运行时所处的供应链和生态系统。随着欧盟《NIS2指令》、网络韧性法案（CRA）、欧盟人工智能法案以及国际自动化学会（ISA）和国际电工委员会（IEC）62443等监管标准的出台，能源行业的首席信息安全官在应对上述潜在影响的同时，必须遵守这些新兴的法规要求。此外，上文所述的地缘政治趋势以及国家与黑客团体结盟的增加，也不断影响数字产品的安全，使关键基础设施面临更大的攻击威胁。首席信息安全官必须为这些发展变化做好准备，并及时调整其应对策略。

主要挑战

数据管理和隐私

能源行业的智能设备为预测性维护和能源优化等功能提供了大量数据集。然而，这些设备通常缺乏统一的安全标准，其身份验证和加密功能较弱，更容易遭受未经授权的访问和数据操纵，从而为企业带来隐私风险和合规挑战。

现有系统和智能产品之间的互通与融合

许多能源企业使用的传统系统并未考虑与互联网连接或与现代智能技术集成。因此，当使用物联网设备和智能产品对此类系统进行强化时，可能会暴露安全漏洞。此外，可再生能源技术的使用增加了系统的复杂性，使网络安全问题更加突出。

生命周期和第三方产品安全

确保智能仪表和电网传感器等互联设备在其整个生命周期中的安全性和韧性至关重要。然而，能源行业对庞大供应链的依赖导致风险上升，因为第三方产品的漏洞可能会危及整个系统的安全性。

主要机遇

- **数据收集和效率**——智能产品的广泛应用不仅提高了效率、服务质量和可靠性，还能够收集、分析和利用更多数据，为运营和客户带来益处。
- **预测、维护和需求预估**——物联网传感器可以实时监控设备并分析运营数据，从而及早发现问题。这有助于减少服务中断时间、降低维护成本，并延长资产寿命。在需求预估方面，智能技术可以通过分析模式和趋势，优化资源分配、电网管理和可再生能源的融合利用，从而实现供需平衡。
- **监管机遇**——欧盟《NIS2》指令和网络韧性法案等法规将更严格的安全标准、风险评估和合规性列为强制要求，从而加强智能设备的网络安全。此类要求将推动企业实施安全设计原则，同时提高供应链的整体安全性。在智能电网和工业物联网等关键基础设施中运行的设备必须符合与安全通信、补丁安装和事件响应相关的严格标准。

能源企业正积极采用智能技术，以提高效率、可持续性和运营可靠性。例如，利用区块链和Web3技术实现去中心化的能源系统，并促进点对点能源交易。电网运营商也在智能电网技术方面进行战略投资。他们通过部署先进的传感器、实时数据分析技术和需求响应系统，优化能源分配并融合利用可再生能源。

此外，企业也纷纷使用智能传感器、物联网设备和先进隔热材料打造节能建筑，以最大限度地减少能源消耗，降低对化石燃料的依赖，并减少碳排放。这些尖端技术使公用事业和消费者得以增强对能源使用的控制，从而改善电网运营并降低成本。

3 韧性设计：为企业与社会提供网络安全保障

由于能源企业日益依赖物联网和运营技术系统，且工业控制系统面临日益复杂的网络威胁，这些企业中负责关键基础设施和资源的首席信息安全官因此面临多重挑战。企业应认识到，大规模业务中断可能危及人类生命安全并造成数据安全风险。监管机构加强对企业关键基础设施安全性和韧性的监管审查，这使得本已艰巨的挑战更加复杂。

在基础设施安全备受威胁的情况下，例如数据采集与监视控制系统（SCADA）破坏、电网攻击和管线中断等，该行业的运营连续性经受着严峻的挑战。为了维持韧性，首席信息安全官必须实施网络安全战略，优先防止业务中断并确保业务在事故发生后能迅速恢复。这包括开展实时监控、攻击面管理、事件响应计划，以及在团队中倡导韧性为先的文化。

不断演进的监管环境，特别是欧盟《NIS2》指令以及北美电力可靠性公司关键基础设施保护标准的实施，提升了对通过强有力网络安全措施保护物理和数字资产安全的要求。将韧性列入工作重点有助于能源企业减少漏洞，并在面对复杂网络威胁时保持稳健运营。

首席信息安全官可据此定位为战略业务推动者，致力于帮助企业提升业务韧性和竞争力。

主要挑战

数字化转型风险

通过将原有的运营技术系统连接到互联网以推动数字化转型，这些通常安全性不高的系统会面临来自互联网的威胁。此外，物联网设备在能源系统中的部署（例如海上风电场和电网的智能电表、远程传感器等），显著扩大了能源系统的攻击面。这些设备通常缺乏有效的安全措施，因此容易被攻击者利用。此外，设备互联还可能引发连锁故障，使事故控制变得更加困难。

可再生能源基础设施安全问题

由于可再生能源基础设施的许多组成部分都提供了数字接口用于远程监控，因此存在安全问题。支持Wi-Fi的物联网设备的加入也使这一问题更加复杂。

纷繁复杂且不断演变的运营韧性法规

由于缺乏统一的区域和国际网络安全标准，能源企业难以确保合规，尤其是关键基础设施提供商。对于跨国企业而言，应对不同司法管辖区之间相互矛盾或重叠的法规，增加了合规的复杂性。违规可能会使其面临巨额罚款、声誉受损以及更严格的审查。

主要机遇

- **实时监控**——使用安全信息和事件管理（SIEM）系统以及入侵检测与预防系统等先进威胁检测工具至关重要。在信息技术和运营技术环境中利用机器学习、人工智能识别和预测恶意行为，可以更快地识别和应对网络威胁。

- **监管发展**——欧盟《NIS2》指令等法规对行业合作和第三方风险管理提出了具体要求。这些法规要求企业控制供应链风险，因此监控关键供应商的网络安全状况势在必行。与其他企业以及政府机构共享威胁情报并进行合作，可以帮助能源企业更好地应对新兴网络威胁。与值得信赖的网络安全供应商建立合作伙伴关系，也有助于快速响应并为事件处理提供支持。

- **网络安全意识和危机模拟演练**——在现代网络韧性培训中，可利用虚拟现实（VR）技术实施沉浸式危机模拟演练，利用人工智能驱动的自适应场景开展个性化学习，以及利用游戏化平台帮助员工和运营商开展交互式事件应对演练。这有助于增强企业的反应能力和运营韧性。

  能源企业作为重要的基础设施提供商，在应用新技术方面应小心谨慎。

- **探索网络风险保险的价值**——随着网络安全威胁的扩大，企业应投入时间了解网络安全保险可以覆盖的风险范围。企业可以设法确定第三方服务中断可能造成的损失，并通过降低服务费率、购买保险或提出诉讼来减少影响。

业界切实应对网络安全问题

积极识别风险并打造能在重大网络事件发生后快速恢复运营的能力，仍然是业内首席信息安全官关注的一大领域。

挑战

一家能源分销商委托毕马威帮助其打造在最严重的网络安全问题出现后迅速恢复运营的能力，并开发用于重新评估其最关键业务应用程序的工具。项目的主要目标是为客户提供一份详尽的手册，其中包含在信息技术系统完全瘫痪情况下应遵循的详细流程、程序和分步指导。此外，还需帮助客户构建用于识别其最关键业务流程的方法。

措施

毕马威的团队与客户的主要业务利益相关方展开合作，深入了解其既有的内部恢复流程。凭借深厚的行业知识和经验，我们为客户精心编制了上述手册，并制定了从零开始逐步恢复信息技术系统的可行流程。

此外，我们还为客户设计并开发了一款工具，使其能够重新分类自己的关键业务应用程序。由于客户之前用于分类应用程序的标准已经过时，导致部分应用程序被错误地归类为关键业务应用程序。这款新工具可帮助客户评估商业影响分析（BIA）中收集的数据，以便重新对其应用程序进行重要性排序。

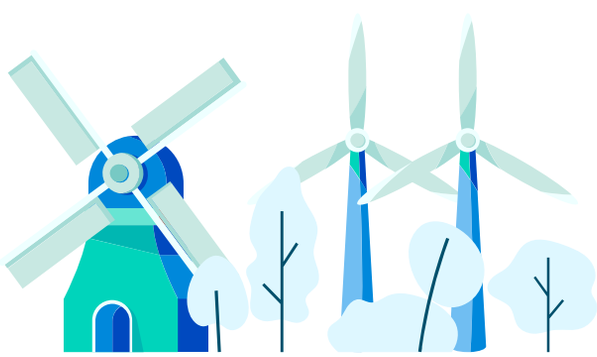
回报

此次合作使客户在信息技术系统全面瘫痪后能够通过流程减少业务中断时间和损失。另外，客户对其业务应用程序和流程的重要程度有了更清晰的了解，从而能够更好地为抵御网络威胁做好准备。

由于存在大范围的供应链以及相互连接的信息技术和运营技术系统，网络安全必须始终放在首位。在缺乏有效防护措施的情况下，迅速采用新技术可能会增加系统漏洞的风险，使企业成为网络攻击的目标。而能源企业在应对此类问题方面正日益成熟。他们通过人工智能和机器学习开展预测性维护和威胁检测，利用区块链确保安全交易，通过高性能计算和物联网进行实时监控，并通过安全设计原则提高安全性。此外，云安全解决方案和集中式网络安全治理还可以帮助企业有效管理和保护数据。

业界专业人士的首要任务

- 明确并加强网络安全治理中的职责，理顺授权范围与领域划分。
- 打破信息技术团队、安全（物理和网络）团队以及运营技术团队之间的壁垒，使各方全面了解自身所面临的威胁态势、所处的组织环境以及相关的供应链情况，并协调提升应急与事件的响应能力。
- 建立覆盖信息技术和运营技术的广泛风险管理框架，并将网络安全风险视为业务风险的一部分。
- 实施兼顾物理风险和网络安全风险的业务连续性和容灾（BCDR）策略。按照现实场景对这些策略进行全面测试和演练。
- 审视保险的覆盖范围是否包括第三方服务中断风险，以确定能否借此降低财务损失。



毕马威可提供的专业服务

毕马威的专业团队能够协助能源行业的首席信息安全官在不断演变的网络安全环境中应对复杂挑战。凭借深厚的行业知识和网络安全专长，我们能够根据企业的独特业务重点和风险状况，量身定制网络安全应对措施。

我们与首席信息安全官紧密合作，制定覆盖信息技术与运营技术的融合、合规、漏洞管理及事件响应等领域的全面战略，充分满足企业的网络安全需求。借助先进的方法论和工具，我们能够评估企业当前的网络安全态势，识别不足和漏洞，并为其设计适应性更强的运营韧性解决方案。

毕马威致力于为企业提供值得信赖的网络安全咨询服务，通过战略方法助力企业挖掘业务价值并获得竞争优势。

毕马威中国联系人

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
科技咨询服务
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

郝长伟
科技咨询技术风险管理服务
主管合伙人
毕马威中国
danny.hao@kpmg.com

黄芃芃
科技咨询技术风险管理服务
业务合伙人
毕马威中国
quin.huang@kpmg.com

kpmg.com/cn/socialmedia

如需获取毕马威中国各办公室信息，请扫描二维码或登陆我们的网站：
https://home.kpmg/cn/en/home/about/offices.html

刊物名称：2025能源行业网络安全重要趋势
刊物日期：2025年6月