

网络安全和信息化与战略管理之问题思考

魏波涛¹ 陈嘉润² 杨振华³

1. 克州党委政法委 新疆克孜勒苏柯尔克孜自治州 845350

2. 汕尾市政府网站管理中心 广东汕尾 516600

3. 云南金鼎锌业有限公司 云南怒江 671401

【摘要】网络安全和信息化建设与战略管理密切相关。信息化的快速发展使组织面临着日益复杂的网络安全风险，而有效的网络安全和信息化战略可以提高组织的安全性、效率和创新能力。整合网络安全和信息化战略，可以确保在信息化建设中兼顾网络安全，提高整体安全性和业务效率，并加强组织的创新能力。此外，网络安全和信息化建设还要求加强信息资产保护，保障重要数据和知识产权的安全，维护组织的声誉和信任。加强风险管理、应急响应能力也是重要的要求，以及时应对潜在的网络安全事件，并最大限度地减少对组织的影响。

【关键词】网络安全和信息化；战略管理；问题思考

引言

随着信息技术的迅速发展和普及，网络安全和信息化建设已经成为组织发展、战略管理不可忽视的重要议题。在信息化的浪潮下，组织不仅面临着日益复杂的网络安全威胁，而且需要合理利用信息化技术来提升运营效率、优化业务流程、实现创新增长。然而，网络安全和信息化建设与战略管理之间存在一系列重要问题需要深入思考。

1 网络安全融入战略规划和决策过程的必要性

首先，网络安全的融入能增强组织的整体风险管理能力。随着数字化时代的到来，网络威胁与日俱增。仅仅依靠防御性的安全措施已经不够。将网络安全纳入战略管理中，可以使组织从全局的角度来审视和应对各种安全风险，通过管理控制和有效资源配置来最大程度地降低潜在风险。其次，将网络安全纳入战略管理可以提高组织的响应能力和灵活性。在不断变化的威胁环境下，仅仅依赖一套固定的防御措施是不够的。战略管理的优势在于它能够使组织更具敏捷性和应变能力，充分考虑到网络安全风险，及时调整和更新战略目标和决策方案，以适应不断变化的威胁形势。最后，将网络安全纳入战略管理对组织的长期发展至关重要。如今，网络安全已经不再是一个仅限于IT部门的问题，而是涉及到组织各个层面的战略性议

题。通过将网络安全融入战略规划和决策过程，可以使组织在数字化转型的道路上更好地把握机遇，管理风险，确保信息安全，实现持续增长和创新。综上所述，将网络安全纳入组织的战略管理中具有重要必要性。只有将网络安全视为组织策略和目标实现的一部分，才能更好地应对威胁，提高组织的抗风险能力，并取得持久竞争优势^[1]。

2 网络安全和信息化建设对加速发展对战略管理的现实要求

2.1 整合网络安全和信息化战略

首先，整合网络安全和信息化战略可以确保在信息化建设过程中兼顾网络安全。信息化建设往往涉及大量的数据、网络和系统的使用和传输，因此网络安全必须成为信息化战略的核心要素。通过整合两者的战略，组织能够更好地识别和分析信息化中的安全风险，并在设计和实施信息化系统时采取相应的安全措施。其次，整合网络安全和信息化战略可以提高组织的整体安全性和业务效率。网络安全和信息化战略本质上都是为了支持组织的业务目标和发展需求。通过整合两者的战略，组织可以在保障网络安全的同时，更好地构建高效的信息化系统和流程，提高业务处理的效率和质量，为组织的加速发展提供坚实的技术支持。最后，整合网络安全和信息化战略可以加强组织

的创新能力。随着信息技术的快速演进，组织需要不断创新和采用新技术来推动业务的发展。通过整合网络安全和信息化战略，组织能够更好地识别和评估新技术带来的安全风险，并在创新过程中采取有效的措施来保护系统和数据的安全。

2.2 强调信息资产保护

首先，信息资产保护是保障组织可持续发展的基础。信息资产的完整性、可用性和保密性对于组织的正常运营至关重要。网络安全和信息化建设需要重视信息资产的保护，通过技术手段和管理措施确保信息资产不受恶意攻击、非法获取或损坏。其次，信息资产保护是合法合规的要求。在现代社会，有许多法律法规和行业标准要求组织保护用户隐私、数据安全和知识产权等信息资产。战略管理需要确保组织严格遵守相关法律法规，制定和执行信息资产保护的政策和措施，以防范法律风险，并避免可能的法律纠纷和损失。同时，合理利用信息资产也可以为组织创造更大的价值和竞争优势^[2]。

2.3 加强风险管理与应急响应能力

首先，加强风险管理是网络安全和信息化建设的重要环节。在制定战略和实施信息化项目时，战略管理需要对潜在的网络安全风险进行全面评估和分析。这包括识别可能面临的威胁和漏洞，评估其影响和可能造成的损失，并制定相应的风险应对策略。通过合理的风险管理，组织可以及早发现和应对潜在的风险，避免或减少安全事件对组织造成负面影响。其次，加强应急响应能力是战略管理的必要要求。即使在加强风险管理的情况下，安全事件仍然可能发生。战略管理需要建立健全的应急响应机制，即时响应并有效遏制安全事件的发展。这包括建立专门的安全团队或机构，培养专业的安全人员，建立有效的检测和监控系统，以及制定应急预案和演练等。在应急响应过程中，战略管理需要迅速采取行动，协调各方资源，及时控制和修复损失，最大限度地减少安全事件对组织造成的影响。加强风险管理与应急响应能力可以提高组织对网络安全风险的防范和控制能力，保障信息系统和数据的安全性

和可靠性。

2.4 提升组织的数字化转型能力

首先，网络安全是数字化转型的基石。随着组织大量依赖互联网和数字技术进行业务运营，网络安全风险也愈发突显。数字化转型要求组织建立安全的信息基础设施，并制定合适的网络安全策略，以保护组织的重要数据、知识产权等信息资产。通过加强网络安全建设，组织能够有效地预防和应对网络攻击、数据泄露等安全事件，确保数字化转型过程的安全性和可靠性。其次，信息化建设提供了实现数字化转型的技术基础。信息技术的先进应用可以帮助组织实现业务流程优化、数据分析、创新产品和服务的开发等目标。数字化转型要求组织充分利用信息化技术，建立数字化的业务模式和运营机制，提升组织的效率、灵活性和创新能力。总之，网络安全和信息化建设对加速发展对战略管理提出了提升组织的数字化转型能力的现实要求。通过加强网络安全、利用信息技术和培养数字化人才，组织能够更好地适应数字化时代的变革，实现持续的竞争优势和可持续发展^[3]。

3 战略管理促进网络安全和信息化有效结合的策略

3.1 将网络安全纳入战略规划

首先，明确网络安全的战略目标。在制定组织的战略规划过程中，将网络安全纳入考虑范围，明确网络安全的战略目标与组织的长期发展目标相一致。这样可以确保网络安全得到充分重视，并避免在信息化进程中出现安全漏洞。其次，建立完善的网络安全策略。基于战略规划，制定具体的网络安全策略。这些策略应涵盖安全架构设计、风险评估和管理、安全培训等方面。通过制定明确的策略，可以指导信息化建设中的网络安全工作，有效减少潜在风险和漏洞。最后，建立信息安全管理体系。引入国际认证的信息安全管理体系（如ISO 27001），通过制定相关政策、风险评估、持续监测与改进等措施，确保网络安全管理得到系统化、规范化的进行。该管理体系的建立可以使网络安全成为组织战略实施的一部分，并有助于与信息化的有效结合。

3.2 加强组织内部的安全文化建设

首先，培养安全意识。通过定期的培训和教育活动，向组织成员传达网络安全的重要性和风险意识。让他们了解常见的网络威胁，提高对个人隐私和信息资产的保护意识。这可以帮助他们理解网络安全是组织发展的基石，从而更加积极地参与到保护网络安全的行动中。其次，强调安全责任。明确每个成员在网络安全方面的责任和角色，使其坚守安全职责。建立安全责任制度，确保每个人都清楚自己在保护信息安全方面的义务。为此，可以制定详细的安全政策和操作规范，并定期进行检查和审查，以确保其执行情况。最后，建立积极的沟通和合作氛围。鼓励组织内部各部门之间的良好沟通和合作，确保网络安全工作与信息化的推进相互配合。建立跨部门的安全委员会或定期召开安全会议，分享经验和最佳实践，加强安全意识的传播和共识的形成。通过加强组织内部的安全文化建设，可以提高组织成员对网络安全的重视程度，并激发他们主动保护信息资产的意识和行动。这有助于促进网络安全和信息化的有效结合，确保组织在信息化过程中的安全和稳定。同时，建设良好的安全文化也是提升组织整体抗击网络威胁能力的关键因素之一^[4]。

3.3 加强与信息技术部门的合作

战略管理在促进网络安全和信息化有效结合方面，加强与信息技术部门的合作至关重要。建立跨部门沟通机制。通过定期召开会议、建立沟通渠道等方式，促进信息技术部门与其他部门之间的密切合作与沟通。这将有助于及时了解各个部门的需求和要求，从而更好地协调网络安全

措施和信息化发展。共同制定网络安全策略。信息技术部门应与其他部门紧密合作，共同制定网络安全策略。深入了解业务需求、风险评估和合规要求，制定相应的安全措施和政策，确保网络安全在信息化过程中得到充分考虑和实施。最后，定期评估和改进。建立网络安全绩效评估机制，定期检查和评估网络安全措施的有效性。信息技术部门与其他部门应共同参与，分析评估结果，并进行必要的改进和调整，以不断提升网络安全水平和信息化效果。

4 结语

网络安全和信息化对战略管理提出了重要的问题思考。在信息化快速发展的时代，组织需要认识到网络安全风险对战略目标造成的潜在威胁，并采取措施加强风险管理应急响应能力。只有确保信息资产的安全与可靠，才能实现战略目标的顺利推进。因此，将网络安全与信息化战略紧密结合，成为组织战略管理的关键一环，以使组织在竞争中获得持续发展和创新的优势。

参考文献：

- [1] 鲁冰, 黄付庆, 王军. 网络安全和信息化与战略管理之问题思考 [J]. 信息安全与通信保密, 2021 (12): 70-76.
- [2] 曹宏亮. 企业信息化建设中网络安全管理问题的思考 [J]. 信息与电脑(理论版), 2019, 31 (17): 218-219+222.
- [3] 崔凯. 对企业信息化建设中网络安全管理问题的思考 [J]. 电子测试, 2018 (12): 122-123.
- [4] 李全忠, 王东升. 对企业信息化建设中网络安全管理问题的思考 [J]. 中国管理信息化, 2017, 20 (10): 66.