湖北网络安全风险评估报告编写编制公司

产品名称	湖北网络安全风险评估报告编写编制公司
公司名称	河南世耀诚实业集团有限公司
价格	.00/件
规格参数	品牌:融河矩媒 服务项目:文案定制 服务方向:专业领域
公司地址	南阳市卧龙区工业路华龙广告二楼
联系电话	13140513661 18338218580

产品详情

网络安全风险管理是指识别、评估企业网络信息系统中的缺陷和风险隐患，并采取相应的安全控制以防止网络威胁，这是一个持续的过程，会随着威胁的发展而不断优化调整。网络安全风险管理和网络安全防护是两个密切相关但不可互换的概念，网络安全防护侧重于应对攻击和响应正在发生的安全事件，而网络安全风险管理则强调从更全面的视角去评估企业的安全状况和面临的威胁态势，要从对组织运营、商誉、财务和合规等多个方面整体应对各种可能发生的网络威胁。

因此，当企业组织开展网络安全风险管理时没有捷径可走，安全团队需要全面考虑各个方面的风险因素。本文梳理了可以有效落地网络安全风险管理流程的10个关键要素，将帮助企业更好开展相关工作。

1、从业务发展的角度识别风险

企业的安全团队应该准确理解，开展网络安全风险管理是为了更好地实现业务发展目标，因此网络安全风险管理的基础要求是要从业务发展的角度识别风险，了解当前网络安全风险的业务环境。从业务发展视角识别现有的安全风险和潜在的安全威胁至关重要，这将决定后续的风险管理工作中需要做多少，以及需要保护的重点是什么。

2、网络安全风险评估

网络安全风险评估是指企业根据其关键业务发展目标，量化不同网络风险的潜在影响以及发生的可能性。通过风险评估，企业管理者和安全团队可以更加合理地分配防护资源，聚焦于关键性风险，以比较具性价比的方式将风险控制在企业可以接受的范围内。网络安全风险评估可以借助FAIR等风险量化模型来实现，主要步骤包括风险范围界定、风险识别、风险分析、风险评估和记录报告等。

3、定义组织的风险承受能力

除了网络安全风险评估，安全团队还必须确定组织的网络安全风险承受能力。当不影响业务发展的时候，企业组织可以接受和承担一定程度的网络安全风险。如果经过量化评估的网络安全风险在可承受的范围内，企业的管理者就可以在一定时期内接受该风险，而将注意力和防护资源投入到更需要重视的高优先级风险中。需要强调的是，企业在定义网络安全风险承受能力的时候，应该与组织的整体业务发展目标保持一致。

4、制定风险化解策略

有许多途径、方法和工具可用于帮助企业管理和缓解网络安全风险，但没有一种策略能够适合所有企业，也没有一种安全工具可以解决所有的问题。企业应该根据已识别风险的关键特征，制定适合自己的风险化解策略，这些策略可能包括实施技术控制措施、流程改进和安全培训计划等。同时，安全团队应该利用先进的安全技术工具，向企业管理层表明降低风险的必要性和价值，并确定风险缓解措施的优先级。

5、制定事件响应计划

没有绝 对的安全，因此企业不能在网络安全事件发生时才被动响应，而是要提前制定安全事件响应的策略和计划，尽量减少攻击事件造成的影响。在此计划中，组织应该明确界定事件响应团队成员的角色和职责，并定期进行演练和演习，测试计划的有效性，并对过程中所发现的不足进行完善。

6. 模拟测试和演练

实战化背景下的模拟测试可以更快速了解企业在网络防御方面的不足，同时梳理企业的IT资产、寻找漏洞和攻击路径，以便更好地修复或应对风险。此外，定期开展测试演练，作用不仅仅在于发现安全问题，对系统开发人员深入了解计算机系统也会大有帮助。通过了解为企业效力的“ 坏人 ”的想法，有助于防止一些灾难性的网络安全事件发生，降低企业业务发展风险。

7. 持续风险监控

网络安全风险管理是一个整体性工作，也是一个持续的流程。实现持续地网络安全风险监控对于发现新的威胁和漏洞至关重要。企业应该积极利用自动化技术，将其量化预警信息或风险暴露状况统一整合起来，提升企业预测潜在风险的能力。实现控制环境与未知风险之间的协同，是开展网络安全风险管理的核心关注点之一。

8. 员工安全意识培养

尽管存在种种技术漏洞，但人依然是网络安全中比较薄弱的环节。企业可以限制用户对某些系统和数据的访问，却难以阻止员工可能会犯的每个人为性错误。因此，持续的员工网络安全意识培训是减小数字攻击面比较重要的安全控制之一。现代企业中的每一位员工都应该定期接受网络安全意识培训，以识别网络钓鱼等攻击企图，了解哪些数据很敏感，了解潜在的风险和漏洞，并了解如何遵循确保敏感数据安全的良佳实践。尽管人为性错误难以避免，但能通过适当的教育和培训，可以大大降低导致数据泄露危害发生的可能性。

9. 供应商和第三方风险管理

随着软件供应链攻击的不断加剧，企业网络安全风险管理不仅需要包括组织内部的管理，还需要定期评估第三方供应商和合作伙伴的安全风险。因为，今 天的企业组织大量依赖于第三方生态来共同构建产品，并完成对用户的服务交付，创建一个有效的TPRM计划对于组织评估潜在的安全风险，管理不断增长的数字攻击面至关重要。

10. 面对管理层的汇报与沟通

网络安全风险管理已经成为企业数字化发展中的核心职能，董事会和管理层对这项工作的关注和审查力度也大大增加。高层领导想知道威胁发生的情况、投入资金的方向以及如何继续改进和发展。因此，安全领导 者需要能够清楚地阐述与业务目标紧密相关的网络安全风险管理计划，避免使用技术术语。此外，要让所有利益相关者都可以及时了解组织在网络安全方面的计划和变动，安全领导
者应该基于新的风险信息编制完整的风险管理态势报告。