# 企业网络安全管理体系的构建与实践

王赞豪
中国电建集团北京勘测设计研究院有限公司　北京　100024

**摘　要：**文章对企业网络安全管理体系建设和实践进行了深入探究。鉴于网络安全威胁形势严峻，本文首先对企业所面临的外在与内在网络安全风险进行分析，指出其风险发展趋势。然后，文章从框架设计、策略规划、组织人员和技术防护这四个方面，详细描述了企业网络安全管理体系的构建过程。本文还重点强调该管理体系在实际工作中的运用，其中包括实施步骤及效果评价。最后总结了主要研究结论，提出网络安全管理体系今后发展趋势及研究趋势。本论文的研究既对企业网络安全管理体系的建设与完善具有理论指导与实践参考作用，又对网络安全领域发展做出新思路。

**关键词：**企业网络安全；风险分析；管理体系构建；技术防护

## 引言

数字化和网络化背景下企业网络安全管理更加重要。在信息技术快速发展的今天，企业对网络系统的日常经营与数据管理的依赖程度不断提高。但是网络安全威胁日益增多与复杂化，对企业构成极大挑战。外部威胁如黑客攻击，恶意软件和钓鱼，内部漏洞如员工操作不规范，系统配置不合适等，均会给企业网络安全带来严重影响。所以，建立完整的网络安全管理体系已是企业的当务之急。这类系统可以帮助企业对各类网络安全风险进行有效的防范，发现与处理，保证企业网络系统具有机密性，完整性与可用性。与此同时，网络安全管理体系也可以增强企业安全意识与应急响应能力，从而为企业稳定发展提供强有力的保障。本次研究以探索企业网络安全管理体系建设及实践为目的，通过对企业网络安全风险进行分析，设计管理体系框架，探索技术防护手段以及实践应用，以期对企业构建科学，实用，有效的网络安全管理体系起到借鉴与引导作用。该研究不仅对于企业网络安全管理有实际意义，而且为网络安全领域发展贡献新思路、新方法。

## 1 企业网络安全风险分析

### 1.1 充分了解网络安全风险

网络安全风险作为信息时代困扰企业的重大问题，背后有着复杂而多变的科技与社会因素。这些风险并不只是技术层面上的漏洞或者外部攻击，而是一个和企业日常经营，员工行为甚至整个市场环境都息息相关的复合体。在网络安全形势越来越严峻的今天，企业有必要对这些风险有一个全面而深刻的了解，从而为建立一套行之有效的安全管理体系奠定坚实的基础。网络安全风险是隐蔽的，突发的，破坏性的。隐匿性意味着许多潜在的安全风险在没有被触发之前是难以被察觉的，这些风险可能隐藏在系统的某个隐蔽角落，等待着合适的时机来触发。突如其来的情况意味着，当这些风险被触发时，它们通常会在很短的时间内产生巨大的影响，给企业带来意想不到的损失。而且破坏性直接表现为网络安全风险严重威胁着企业的正常经营与信誉。

### 1.2 企业内外网络安全风险相互交织

我们在讨论企业网络安全风险问题时，必然要分清外在与内在两大类别。外部风险则主要来自网络中存在的黑客攻击，恶意软件和钓鱼网站等多种威胁。这些攻击策略变得越来越狡猾和复杂，它们针对企业的弱点，试图窃取敏感信息、破坏系统或勒索金钱。比如最近几年频繁出现的勒索软件攻击，是通过加密手段将企业数据进行锁定，进而要求商家支付高额赎金。但内部风险也是不可忽视的。在许多情况下，企业网络安全漏洞并不是来自外部攻击，而更多是由于内部员工操作不当或者疏忽大意造成。例如，一名雇员可能会无意地点击钓鱼邮件的恶意链接，从而使恶意软件散布到企业网络上，也可能是某部门系统管理员未及时对系统补丁进行更新而让黑客有机可乘。另外，由于远程办公及移动设备的广泛使用，企业网络边界日益模糊，也对企业内部安全管理提出了全新的考验。

### 1.3 风险趋势动态演化

网络安全风险并不是一成不变。与此相对，它们会随着技术进步和市场环境的转变而持续发展。一方面是新型攻击手段与漏洞使用方式不断涌现，如使用人工智能技术实现更加准确的网络钓鱼或使用物联网设备漏洞实施大规模网络攻击等。另一方面伴随着企业业务数字化，云化趋势的加快，数据泄露，系统瘫痪的风险越来

越大。所以企业对网络安全风险进行分析时一定要保持能动的目光，随时注意最新的安全威胁与漏洞信息，并对其安全策略与防护措施进行适时的调整。还要强化员工安全意识与技能培训以提升其风险防范与应对能力。唯有如此，才能够使企业在网络安全环境越来越恶劣的情况下立于不败之地。

## 2 企业网络安全管理体系的建设

### 2.1 构建网络安全管理全方位体系框架

在企业网络安全管理体系建设中，必须先设计出全方位，多层次框架来保证系统的完整有效。该框架既考虑到了技术层面上的保护，又涵盖了组织，人员和过程等诸多层面。在网络安全管理体系中，技术防护占据着基石地位。通过防火墙，入侵检测系统的部署以及数据加密的技术手段能够有效地抵抗外部攻击以及内部泄露。但是技术不是万能的，还要辅之以合理的组织结构、人员配置等。比如成立专门安全团队或者职能部门处理网络安全事务、厘清各岗位权责、避免安全管理真空地带等。另外，流程是网络安全管理体系必不可少的环节。从安全事件发现，上报，应对到处理，各个环节均需制定清晰的程序与标准。这既可提高安全管理效率，又可在关键时刻快速作出正确决策与行动。

### 2.2 制定科学，合理的网络安全策略和方案

网络安全策略和规划是引导企业网络安全的纲领性文件。企业制定上述战略需充分考虑其业务特点，安全需求及风险承受能力。一是确定安全目标。企业网络安全目标应以保证业务连续性，数据机密性与完整性，系统可用性为目标。围绕上述目标，具体安全原则与规范可进一步提炼，例如最小权限原则，数据分类保护等等[1]。二是综合安全需求分析。其中包括企业原有网络系统脆弱性评估，潜在安全威胁预测，法律法规与合规要求解读等。通过对其进行分析，使企业能够清楚认识到自身在网络安全问题上的空白与不足，以便制定出具有针对性的改善措施。最后应把这些战略和计划付诸实施。其中包括确定执行时间表，负责人员，必要资源和预期结果。唯有如此，网络安全策略才可以保证不流于形式，而能实实在在地落地实施。

### 2.3 打造高效协同的网络安全组织与人员队伍

任何一个管理体系要想取得成功，都必须要依靠人这一要素。组织与人一样对网络安全管理体系起着关键作用。一是构建高效协同的网络安全组织。该机构应具有跨部门和跨层级协调能力并能第一时间处理安全事件。同时也要明确各部门、各岗位对网络安全工作的责任与划分，避免推诿扯皮。二是加大网络安全人员培训与引进力度。定期开展安全意识教育，技能培训及实战演练等活动，可提升现有工作人员安全素养及应对能力。与此同时，我们也要积极从外部引进网络安全专业人才给企业带来新生与生机。最后是建立完善激励机制与职业发展路径。通过对网络安全人员进行物质与精神奖励及清晰的晋升通道能够调动网络安全人员工作积极性与创新精神。

## 3 企业网络安全技术防护体系

### 3.1 综合运用和整合网络安全技术

在企业网络安全技术防护体系建设中，首先要清醒地看到单一安全技术很难面对复杂多样的网络威胁。所以企业有必要将各种网络安全技术结合起来，实现其深度融合，从而建立起多层次，立体化安全防护网。网络安全技术涉及但不仅仅局限于防火墙，入侵检测系统，数据加密和身份认证。这些技术分别在企业网络中的各个层次，各个环节中发挥作用。比如防火墙作为网络中第一道防线可以滤除大部分恶意流量及攻击。入侵检测系统具备实时监测网络中异常行为的能力，能够迅速识别并处理可能的安全风险。通过数据加密和身份验证技术，我们可以确保数据的保密性和完整性，从而避免敏感信息的泄露或篡改。但是，这类技术并非孤立的存在。为了构建一个高效的安全防护体系，它们之间必须进行紧密的合作和共同努力。比如防火墙能和入侵检测系统一起工作，在发现流量不正常的情况下自动屏蔽。

### 3.2 深入部署和不断优化网络防御技术

在网络安全技术防护体系中，网络防御技术占据着核心地位。企业在配置这些技术时需综合考虑其业务特点，网络架构和安全威胁，有针对性地制定防御策略。深入的部署意味着公司必须在网络的每一个细节和地方都融入防御技术。其中既包含了传统网络边界防御问题，也涉及内部网络，终端设备和云环境。比如将入侵检测系统部署到内部网络上，就能及时地发现内部威胁，将安全软件安装到终端设备中，可避免恶意代码。云环境下使用安全访问控制与数据加密技术，能够对云数据安全进行防护。持续的优化策略是确保防御技术能够长期发挥作用的核心要素。由于网络威胁在不断地演化与升级，因此企业有必要对其防御技术做出经常性的评估与调整。其中包括病毒库的更新，安全软件的升级以及系统漏洞的修复。与此同时，企业也需重视最新安全威胁情报与漏洞信息，并适时调整防御策略，才能应对不断产生的安全风险。

### 3.3 网络安全评估与测试的持续进行与结果反馈

网络安全评估与测试，是对网络安全技术防护体系

效果进行测试的一种重要方法。企业通过定期评估和检测，能够了解其安全防护体系中存在的薄弱环节及潜在风险，以便及时采取措施加以改进。网络安全评估是由网络安全策略，安全配置和安全漏洞综合考察组成。在评估过程中可使用的方法与技术有很多，例如漏洞扫描，渗透测试，安全审计[2]。这些方法与技术有助于企业及时发现网络存在的安全漏洞与潜在威胁，并为之后的维修与加固提供基础。网络安全测试实际上是一个针对安全防护体系的实际操作模拟过程。通过对真实网络攻击场景及威胁行为进行仿真，企业能够对安全防护体系实际防护能力及响应速度进行测试。在试验过程中要注意对试验结果进行分析与反馈，掌握试验中所发现的问题与不足之处，及时加以改进与优化。

## 4 企业网络安全管理体系的实践研究

### 4.1 网络安全管理体系实施步骤的详细规划与执行

企业网络安全管理体系实施过程具有系统性和复杂性，牵涉众多环节及部门，所以细致的计划和实施非常重要。企业要有清晰的执行计划，其中包括执行的时间表，必要的资源和关键节点。该方案应根据企业实际情况及安全需求保证执行可行有效。企业在制定方案时，需充分考虑到各种潜在的风险与挑战，事先拟定好应对措施。然后企业要配置必要的资源与执行职责。它包括人力，物力，财力及其他资源，也包括各部门，各岗位执行时的权责。资源配置要按照实施计划需要合理调配，保证资源得到充分利用，避免造成浪费。明确职责，又能确保执行过程各环节衔接顺畅，协调一致。那么企业就需要根据实施计划来循序渐进地构建网络安全管理体系。这一过程涉及部署技术防护手段，制定安全策略，组建安全组织等诸多内容。企业在前进的道路上，需要时刻注意执行的结果与反馈，并对执行策略进行适时调整，以便处理可能遇到的各种问题。最后要求企业在执行过程中不断监测与评价[3]。其中包括监控安全事件，修补安全漏洞和调整安全策略。企业通过不断的监测与评价，能够及时掌握网络安全管理体系运行状况与成效，从而为之后的完善与优化奠定基础。

### 4.2 网络安全管理体系效果评价的全面性与客观性

对网络安全管理体系实施效果进行评估，是对体系建设成果进行检验的一个重要途径。为保证评估的全面性与客观性，企业有必要构建科学、合理的评估指标体系，收集、分析有关数据，为评估结论提供支持。评价指标体系应包含安全事件减少率，安全漏洞修复率和员工安全意识增强度等诸多指标。这些指标能够从不同角度体现网络安全管理体系所取得的成效与贡献。同时指标设置要有可量化、可衡量等特征，以便于企业收集数据、分析数据。从数据采集与分析的角度来看，企业有必要利用各种方法与工具对相关的数据进行采集，例如日志分析，问卷调查以及安全测试。这些资料能够给企业一个客观，真实的评价依据。企业通过深入分析与挖掘数据，能够了解网络安全管理体系中各方面的性能与问题，并为之后的完善指明方向。另外企业需关注评估的持续性与动态性。由于网络安全风险在不断发生变化与演变，因此网络安全管理体系需要不断做出适应与调整。所以企业有必要对网络安全管理的系统进行经常性的评估与审核，以保证系统能时刻保持有效性与先进性。

## 5 结语

本次研究在深入探究企业网络安全管理体系建设和实践的基础上，获得了一系列重要的结论。一是企业网络安全管理体系建设是一项系统性工程，要从技术，组织和人员几个层面进行全面考虑。二是实践是检验管理体系是否有效的惟一标准，需要企业在实践中不断地总结经验教训，不断地对管理体系进行优化与完善。

## 参考文献

[1]郭东华,王庆.解析电力企业信息网络安全风险分析与管控[J].现代经济信息,2020,(05):22+24.

[2]郭磊.中央企业网络安全风险分析和对策[J].上海船舶运输科学研究所学报,2019,42(03):56-61.

[3]曲峰.企业网络信息安全风险分析与设计思路[J].数字通信世界,2017,(12):250.