企业信息安全管理策略研究

沈 磊
上海华测导航技术股份有限公司 上海 201706

摘 要：在数字化浪潮席卷全球的当下，企业信息已成为核心资产，其安全管理关乎企业存亡与社会经济稳定。当前，企业信息安全管理面临技术防护短板、管理体系漏洞及人员安全意识匮乏等困境。为有效抵御网络攻击、数据泄露等风险，需从强化技术防护体系、完善管理架构、提升人员安全素养及建立应急响应机制等方面入手，构建全方位、多层次的信息安全管理体系，保障企业信息资产安全，促进企业可持续发展。

关键词：企业；信息安全管理；策略

引言

随着信息技术的迅猛发展与深度应用，企业运营对信息系统的依赖程度日益加深，信息安全已成为企业核心竞争力的关键组成部分。然而，复杂多变的网络环境与层出不穷的安全威胁，使企业信息安全面临严峻挑战。技术防护不足、管理体系缺陷及人员意识薄弱等问题，导致企业信息安全事件频发。在此背景下，深入研究企业信息安全管理策略具有重要的现实意义。本文将针对现存问题，提出系统性的管理策略，助力企业提升信息安全防护能力。

1 企业信息安全管理概述

企业信息安全管理聚焦于保护组织数字资产的保密性、完整性与可用性，涵盖从数据、网络到应用程序等多维度的安全防护。在数字化转型加速推进的当下，企业运营深度依赖信息系统，各类业务流程、客户数据、商业机密均以电子形式存储和流转，这使得信息安全管理成为企业稳健发展的核心要素。信息安全管理需构建系统化的防护体系，从技术层面来看，通过部署防火墙、入侵检测系统、数据加密技术等，对外部网络攻击和内部数据泄露风险形成有效阻隔。防火墙作为网络安全的第一道防线，能够依据预先设定的安全策略，对进出网络的流量进行过滤和监控，阻止非法访问请求；入侵检测系统则实时监测网络活动，识别异常行为并及时发出警报，以便安全人员采取应对措施；数据加密技术将敏感信息转化为密文，即便数据遭到窃取，未授权者也无法解读其真实内容，从而保障数据的保密性。从管理角度出发，企业需强化人员安全意识，规范操作流程。员工是信息安全的关键环节，不当的操作行为，如使用弱密码、随意点击不明链接等，都可能为企业带来安全隐患。通过开展针对性的培训和教育，使员工深刻认识到信息安全的重要性，养成良好的安全操作习惯。建立严格的访问控制机制，根据员工的岗位职责和工作需求，合理分配数据访问权限，避免权限滥用导致的数据泄露问题。随着云计算、大数据、物联网等新兴技术的广泛应用，企业信息安全管理面临着新的挑战与机遇。第一，新技术带来的复杂架构和开放环境增加了安全风险；第二，也为安全管理提供了更先进的工具和手段。企业需要不断优化信息安全管理策略，引入智能分析、自动化响应等技术，提升安全防护的效率和精准度，以应对日益严峻的信息安全形势，确保企业在数字化浪潮中平稳前行。

2 企业信息安全管理现状分析

2.1 技术防护存在短板

在数字化转型浪潮推动下，企业业务系统与网络环境日益复杂，然而技术防护层面暴露出诸多不足。部分企业部署的防火墙设备仍沿用传统包过滤技术，面对频繁变异的应用层攻击，如SQL注入、跨站脚本攻击（XSS）等，难以实现精准拦截与有效防御。入侵检测与防御系统（IDS/IPS）部署分散且缺乏统一管理，无法及时关联分析各节点日志数据，导致潜伏在网络中的恶意程序或异常行为无法被迅速识别，安全威胁持续存在并可能不断扩散。企业对云计算、大数据等新兴技术的应用，使数据存储与处理边界变得模糊，传统的数据加密技术在云环境下面临密钥管理复杂、数据完整性验证困难等挑战，难以保障数据在全生命周期内的安全性。企业在终端防护环节也存在明显漏洞，移动办公设备、物联网终端等接入网络时，缺乏有效的身份认证与设备合规性检查机制，一旦这些终端设备被恶意软件感染或遭受物理窃取，攻击者便能轻易获取企业内部网络访问权限。企业网络安全监测工具的实时性与准确性不足，无法对网络流量进行深度分析与智能识别，对于加密流量中的隐藏攻击更是难以察觉，导致安全事件发生后无法

快速定位与响应，增加了数据泄露与业务中断的风险。在软件供应链安全方面，企业对第三方组件、开源代码的安全审查存在缺失。大量未经严格检测的开源库被引入开发项目，其中潜在的安全漏洞成为攻击者的突破口。当开源社区发布漏洞补丁时，企业由于缺乏完善的软件更新机制，无法及时对系统进行修复，使得整个信息系统长期暴露在安全风险之下，为数据泄露与系统瘫痪埋下隐患[1]。

2.2 管理体系不完善

企业信息安全管理缺乏系统化、规范化的运作模式，各部门之间职责界定模糊，信息安全工作常出现推诿扯皮现象。在实际工作中，IT部门负责技术层面的安全维护，业务部门关注业务发展，两者之间缺乏有效的沟通与协作机制，导致安全需求与业务需求脱节。例如，业务部门为追求效率快速上线新应用系统，却未与IT部门充分沟通安全防护要求，使得系统上线后存在大量安全漏洞，增加了企业信息安全风险。安全流程的设计与执行存在缺陷，从安全事件的预防、监测到响应与处置，缺乏标准化的操作流程。安全事件发生时，企业往往无法按照既定流程快速启动应急响应，各部门之间的协作混乱无序，导致事件处理效率低下，安全损失进一步扩大。企业对安全流程的执行情况缺乏有效的监督与评估机制，无法及时发现流程中存在的问题并进行优化改进，使得安全管理工作流于形式，难以真正发挥作用。在安全资源的调配与管理上，企业存在不合理现象。过度重视硬件设备的采购，而忽视了安全服务、人员培训等方面的投入。大量资金用于购置高端防火墙、入侵检测设备等，但由于缺乏专业的运维团队与安全服务支持，这些设备无法发挥最大效能。企业在安全预算分配上缺乏科学规划，未能根据实际安全风险与业务需求进行动态调整，导致部分关键安全领域资源不足，而部分领域资源闲置浪费，影响了整体信息安全防护水平的提升。

2.3 人员安全意识薄弱

企业员工对信息安全的重要性缺乏深刻认识，日常工作中存在诸多不安全行为。密码使用方面，随意设置弱密码、重复使用密码现象普遍，账号密码极易被破解或通过社工手段获取。在公共网络环境，员工未经安全评估便直接连接企业业务系统，大幅增加数据泄露风险。处理敏感数据时，员工保密意识欠缺，常通过非安全渠道传输或存储数据，如用个人U盘拷贝企业机密文件、借助公共云盘分享业务数据，一旦设备或平台遭恶意攻击，企业核心数据将面临泄露危机。面对复杂多变的网络攻击手段，员工识别与防范能力不足。钓鱼邮件、恶意链接等社会工程学攻击不断升级，员工难以辨别真伪，不经意间点击或下载，导致设备感染病毒、木马，进而使企业网络遭受攻击。遭遇安全事件时，员工缺乏正确应对方法，未及时上报，反而自行不当操作，如删除可疑文件、关闭报警系统，既无法解决问题，还可能破坏证据，加大安全事件调查与处理难度。企业内部缺乏持续有效的信息安全宣传与教育机制，员工获取安全知识渠道有限，安全意识难以持续提升。新员工入职仅接受简单安全培训，后续缺乏定期复训与考核，对新出现的安全威胁与防护措施了解不足。信息安全未融入企业文化与员工绩效考核体系，无法激励员工主动提升安全意识与行为规范，企业信息安全管理工作难以获得员工积极支持与配合，安全风险防控存在较大缺口[2]。

3 企业信息安全管理策略

3.1 强化技术防护体系

（1）构建多层级网络安全防护架构，在企业网络边界部署下一代防火墙，其集成入侵防御系统（IPS）功能，通过深度包检测技术对进出网络的数据流进行协议分析与特征匹配，精准识别并阻断恶意攻击流量。配合部署高级威胁检测系统，利用人工智能与机器学习算法，实时监测网络中异常行为模式，如横向移动攻击与数据泄露迹象，形成对外部攻击的第一道防线。（2）针对企业内部核心数据，采用加密存储与传输技术。在数据存储层面，使用AES-256等高强度对称加密算法对静态数据加密，确保即使存储介质丢失或被盗取，数据内容也无法被读取。在数据传输过程中，应用TLS1.3协议建立安全通道，对传输数据进行动态加密，防止中间人攻击窃取敏感信息，实现数据全生命周期的安全保护。（3）搭建安全态势感知平台，整合企业内各类安全设备日志与流量数据，通过大数据分析技术实现对企业信息安全状况的实时可视化呈现。该平台可基于历史数据构建正常业务行为基线，实时监控各项操作动态。当检测到偏离基线的操作时，会及时发出预警，并结合威胁情报库，快速定位攻击源头与潜在影响范围，为安全决策提供有力支撑。

3.2 完善管理体系建设

（1）实施严格的访问控制管理，依据最小权限原则，对企业内部员工、合作伙伴及第三方服务人员的系统访问权限进行精细划分。采用基于角色的访问控制（RBAC）模型，为不同岗位设定对应的权限集合，确保用户仅能访问完成工作所需的资源。定期对权限分配情况进行审计，及时清理离职员工与岗位变动人员的多

余权限，降低内部越权操作风险。（2）建立资产全生命周期管理机制，对企业内所有信息资产进行详细登记与分类，明确资产的重要程度与敏感等级。针对高价值资产，制定专门的保护方案，从物理环境、网络安全、数据备份等多个方面进行重点防护。随着技术发展与业务变化，动态更新资产清单与保护措施，确保资产始终处于有效保护状态。（3）加强供应链安全管理，在选择供应商与合作伙伴时，对其信息安全能力进行全面评估，包括安全技术水平、数据保护措施以及安全事件应对能力等。在合作过程中，通过签订安全协议明确双方责任与义务，要求供应商定期提供安全评估报告，对涉及企业核心数据交互的环节进行严格监控，防止因供应链漏洞导致企业信息安全受到威胁[3]。

3.3 加强人员安全培训

（1）开展针对性的安全意识提升活动，通过模拟钓鱼攻击演练、安全案例分析等形式，让员工直观感受信息安全威胁的真实场景。定期组织信息安全知识讲座，讲解常见攻击手段、数据泄露危害以及个人在信息安全保护中的责任，培养员工主动识别与防范安全风险的意识，使其在日常工作中保持警惕，避免因疏忽造成安全漏洞。（2）进行岗位技能专项培训，根据不同岗位的信息安全需求，制定差异化的培训内容。例如，为系统管理员提供网络安全设备配置与漏洞修复培训，使其能够熟练应对各类安全事件；为研发人员开展代码安全编写培训，教授安全编码规范与漏洞检测技术，从源头减少软件安全隐患，提升员工在各自岗位上保障信息安全的专业能力。（3）建立安全行为激励机制，对在信息安全工作中表现突出的员工给予表彰与奖励，如评选“信息安全卫士”等荣誉称号，并给予物质奖励。将信息安全行为纳入员工绩效考核体系，对违反信息安全规定的行为进行相应处罚，形成良好的信息安全文化氛围，促使员工自觉遵守安全规定，积极参与企业信息安全建设。

3.4 建立应急响应机制

（1）制定详细的应急响应预案，针对可能出现的各类安全事件，如数据泄露、勒索软件攻击、系统瘫痪等，明确应急响应流程与各部门职责。预案应包括事件报告流程、应急处置步骤、恢复策略以及对外沟通机制等内容，并定期对应急响应预案进行演练与修订，确保预案的实用性与有效性。（2）组建专业的应急响应团队，团队成员涵盖网络安全专家、系统运维人员、数据恢复工程师等不同领域专业人员。定期组织团队进行应急演练与技能培训，使其熟悉各类安全事件的处置流程与技术手段，确保在安全事件发生时能够迅速响应，采取有效措施控制事态发展，减少企业损失。（3）建立应急资源储备库，储备必要的应急工具与设备，如数据恢复软件、备用服务器、应急电源等。与外部安全服务机构建立合作关系，确保在遇到重大安全事件时能够获得专业的技术支持与资源补充。定期对应急资源进行检查与更新，保证资源处于可用状态，为应急响应工作提供坚实保障[4]。

结语

综上所述，企业信息安全管理是一项系统且复杂的工程，涵盖技术、管理、人员等多个维度。针对当前技术防护短板、管理体系不完善、人员安全意识薄弱等问题，通过强化技术防护体系、完善管理体系建设、加强人员安全培训及建立应急响应机制等策略，能够有效提升企业信息安全防护水平。唯有将这些策略有机结合并持续优化，方能筑牢企业信息安全防线，为企业在数字化时代的稳健发展保驾护航。

参考文献

[1]赵越,马玉伟,韩磊.集团企业一体化信息系统安全管理策略研究[J].军民两用技术与产品,2024(4):66-69.

[2]张婉妮.企业信息安全管理现状与策略研究[J].现代工业经济和信息化,2022,12(1):123-124,127.

[3]董金玉,肖汉,刘石.大数据背景下石油企业网络信息安全管理策略研究[J].中国管理信息化,2023(10):94-96.

[4]姜蒙娜,邵剑飞,王伟业.电力企业网络信息安全管理研究[J].科学与信息化,2024(9):7-9.