对企业信息化建设中的网络安全管理问题探讨

李强生，陈黎

广东南方通信建设有限公司，广东广州，510630

摘　要：为更好地适应现代社会发展的需要，企业应注重技术创新，提高自身竞争力，积极学习现代管理理念，引入多元化管理方法，不断创新，统筹规划，设定长期可行的发展目标并确保公司日常工作的顺利开展。此外，管理者还应认识到建设企业信息化和管理创新对企业发展的积极影响，将现代科技融入日常管理活动，不断提高企业管理工作的质量和有效性，应对复杂的市场环境，以积极的态度，对提升企业整体竞争力起到不可替代的作用。

关键词：企业；信息化；建设；网络安全；管理；问题；探讨

中图分类号：TP393.08;F270.7　　**文献标志码：**A

0　引言

随着信息时代的到来，信息技术已广泛应用于各行各业，促进了社会经济的快速发展，为人们提供了便捷的生活方式。现代企业利用信息技术进行资源管理，使企业能够更快地适应市场经济体制的转变，加快企业管理现代化进程，同时加强企业资源管理。目前，信息技术在商业中的应用还存在一些不足。员工是企业信息系统的直接使用者，内部人员的泄密给企业带来的损失是致命的。因此，在当前的企业网络安全运行维护工作管理过程中，就需要加强对于工作人员的培训教育工作，从思想意识等方面提升员工的自觉性、自律性。

1　信息化与企业管理的关系

企业要想长期稳定发展，就需要管理者充分整合和利用企业内部资源，保证企业资源配置的合理性。特别是在新时期，外部竞争压力增加，企业为了稳固自己的市场地位，应从内部管理出发，积极进行改革创新，并主动学习、获取现代信息技术，利用信息化手段实现产品创新，帮助企业打开市场，为企业成功转型奠定基础。企业信息化建设的最终目的是保障企业各项工作高效运行，而要想实现这一目标就必须构建科学、完善的绩效考核体系，对企业内部人员展开标准化和规范化管理，依托现代化管理方式，将企业信息化建设与管理工作有机结合起来，促进企业全面发展。

2　对企业信息化建设中的网络安全管理中存在的问题

2.1　风险问题

风险分析的重要过程是确定所有需要保护的资源，尤其是与安全性问题相关的资源。这些资源包括：工作站、服务器、网络和其他硬件设备等；程序和应用程序、操作系统和其他软件的在线存储、传输和数据备份。企业网络系统几乎包括所有的开源资源，如果企业尚未构建安全和保护系统，则将存在以下重大安全威胁：①与Internet的直接链接；②脆弱的欺诈行为；③数据漏洞；④缺乏对整个网络安全管理的控制；⑤缺乏防止泄漏的安全措施。

2.2　安全问题

①内部安全问题，包括网段的划分；②如何实现网络边界安全；③如何保证应用系统的安全

性；④如何防止黑客入侵网络和服务器；⑤如何实现数据库和个人终端安全；⑥如何保证企业信息传输安全和计算机网络安全；⑦如何阻止在通讯内容中的否认、伪造、篡改和冒充行为；⑧如何评估整个网络安全系统。

2.3 企业员工缺少安全管理的责任心

目前，在推进企业网络安全运行维护工作的过程中，相关的技术人员是主要的参与者。由于企业网络信息建设中网络安全维护是一项全面而系统的工作，任何细小的环节不到位，都会对整体的工作成果带来直接的影响。部分工作人员在进行网络安全维护工作时，缺少安全管理的责任心，对于网络安全工作的具体内容和工作规范要领掌握不到位，无法第一时间应对和处理网络安全维护工作中的突发事故。在当前的企业内部网络安全维护工作中，人为事件造成损失的概率远远大于系统本身抗风险能力。在实际的操作运行环节，工作人员自身的大意和疏忽，都会对企业网络信息安全运行带来直接的影响。此外，企业内部工作人员之间是有所差异的。

2.4 企业缺少信息安全管理体系

目前，在推进企业网络信息建设中，网络安全维护工作依旧存在着亟待解决的问题。主要问题之一是部分企业缺少信息安全管理制度，制度的缺失对于措施的执行和延续是十分不利的。缺少必要的信息安全管理制度，一定程度上从侧面反映出部分企业管理者，对于网络安全维护工作的不重视。现如今，企业信息安全工作与企业网络信息建设有着千丝万缕的联系，做好基础的网络安全维护工作，才能够更好地发挥企业信息网络建设的整体效用。必要的制度体系，能够在一定程度上推动企业网络安全维护工作的常态化和正规化。

2.5 软硬件安全存在的问题

软硬件技术层面的问题主要表现在网络硬件安全隐患、软件缺陷和漏洞、病毒和恶意程序等。其中，硬件层面的安全隐患方面比较有代表性的是路由器，如果路由器安全性能较低，可能会带来一定的安全问题。企业在生产经营的过程中不可避免地要涉及到操作系统、应用软件，软件或者系统中的缺陷和漏洞将会成为恶意攻击方的着力点。部分网络软件开发商为了便于后续升级，常常设置一定的“后门”，这也为不法分子非法入侵提供了渠道。恶意攻击方基于该通道窃取机密数据和信息，将会给企业带来严重的经济损失。病毒和恶意程序具有传播速度快、影响范围广的特点，大多通过各种渠道入侵到内部网络中，严重者可能造成网络的瘫痪。部分企业安全防护更新速度较慢，难以对各类病毒起到保护作用，是病毒和恶意程序蔓延的重要因素。为了实现资源的实时共享，网络的开放程度越来越高，一方面提升了人们获取信息的便捷度，但另一方面也导致网络遭受攻击的可能性加大。部分用户缺乏安全防护意识，登录口令设计得过于简单，增加了计算机网络遭到非法破坏的概率。

2.6 企业全员参与不到位

企业信息化是一项非常复杂多样的系统工程，随着信息工程的发展和完善，我国大部分的企业为了紧随其他企业的发展速度，在缺乏深入调研的情况下开展信息化建设，对于当下现状、需求、相关信息化等没有充分掌握，特别是在信息化的建设以及企业战略发展当中存在较大的差异，这就导致信息化项目的规划缺乏完善性，存在较大的缺陷。调查需要做到全员调查，如果调研不够深入，问题分析不够透彻，则不能得到满足。同时，没有生产和管理部门的参与，信息化建设的完善度很难提升，系统的应用效果不理想，对企业发展造成巨大阻碍。

3 对企业信息化建设中的网络安全管理探讨

3.1 构建完善的管理体系，规范企业人员行为

要健全企业网络信息服务提供商的管理机制。以相关法律法规为基础健全服务商行为管理机制，防止服务商受利益诱惑使用不正当手段威胁用户数据安全。按照相关法律法规保证

服务商能够自觉遵守自身的义务，使服务商尊重企业自身的知情权、并在企业的数据信息受到不正常攻击时发出通知，确保企业能够收到示警。确保企业自身的知情权能够受到保护。其次，要建立健全企业内网络信息安全管理机制。相关工作人员需要结合国家的相关政策、企业的信息安全要求制定合理的安全管理机制，用以规范企业员工的操作，防止因企业内部人员操作问题给不法分子可乘之机。比如，增强企业员工的安全意识，使其自觉警惕可疑链接、不明来源软件等等。最后，网络安全管理人员需要加大管理力度，坚决贯彻企业内部控制管理条例，将不安全因素控制在摇篮里。定期对员工进行抽查，检查其在信息安全方面的文化修养与实操能力，确保员工都能够掌握计算机系统的安全操作技巧，从根本上保证企业内信息的安全。

3.2 积极推动信息化建设

我国大型企业发展需要提高自身的竞争力，信息化建设作为大型企业进行自身结构调整，提高管理水平，提高效率的主要方式，可以帮助企业更好地突出特色，满足需求。现阶段信息化的改革浪潮为大型企业的信息化建设提供了良好的机会，积极开展信息化建设，可以帮助大型企业在市场上当中站稳脚跟。南钢用三年的时间，2亿元的投资，建设了覆盖全部业务领域的182个子系统，累计实现直接经济效益3亿元以上。通过理念创新、技术创新和管理创新，发挥后发优势，南钢信息化在三年内从行业中游水平跃升到一流方阵，已从跟随转变为跟随与创新相结合。

3.3 利用安全技术，保证企业信息安全

优化传统网络安全技术传统网络安全技术以加密技术、访问控制技术、防火墙技术、入侵检测技术、认证技术为主。大数据时代信息技术更新迭代速度加快，企业内网络信息安全管理人员需要加强对传统技术的创新，确保内部机房环境、视频监控系统、防火墙、入侵防御系统、数据库审计系统、应用交付系统的安全。充分发挥认证技术的优势，设置安全认证系统，只有经过网络安全授权的工作人员才有访问企业内部数据的资格，以防止外部人员对企业内部系统进行攻击。对传统的访问控制进行适当的技术创新，将其应用到企业内部网络资源权限的管理系统当中。通过使用访问控制技术防止外部人员非法获取企业内部的网络信息数据，从而保证企业内部的数据安全。重视传统防火墙技术的应用，在企业内部构建个性化的网络安全屏障，通过阻隔外部的恶意攻击保证企业内网络系统的安全。同时，加强对新型防火墙技术的推广，将网络地址翻译、虚拟专用网、加密技术、身份认证技术等技术应用到企业内安全屏障的设置工作当中，实现对安全系统的优化。使用大数据安全技术使用大数据安全技术能够保障网络信息数据各个生命周期的安全，降低企业遭受病毒攻击的风险。大数据安全技术主要以大数据采集、储存、挖掘、发布、检测攻击等技术为主。将数据源身份认证技术、密文附加消息认证码技术、时间戳等应用到信息数据的采集过程中，能够满足企业人员对信息数据安全传送的基本要求。将隐私保护技术、数据加密技术、密钥管理技术、异地备份技术应用到数据存储过程中，可以满足企业人员对网络信息安全存储的基本要求。将动态口令技术、人脸识别技术、声纹识别技术应用到数据提取过程中，可以避免企业内部信息外泄，造成企业经济损失。制定APT检测方案，可以有效检测出企业存在的内部威胁、欺骗钓鱼、木马后门、SQL注入等安全隐患，保障企业内部大数据的安全。

3.4 提高网络安全整体把控力

推进网络安全工作的过程中，任何环节都要做到精准把握。构建整体的框架体系，要细化内部的系统，做到衔接。基于Agent的NSSA在进行态势量化的过程中，主要针对的是整个网络，其感知的是知识库中被提取出的安全事件信息。在这其中，主要运用数据通信技术。该技术是通信技术和计算机技术相结合的新型通信方式，实现了信息通信的新高潮。从数据的采集到数据的预处理、从态势的量化到态势预测，Agent改进

模式的NSSA架构体系让当下的网络安全得到了进一步的提升。充分发挥系统内部各子系统的优势，让技术的力量发挥到最大，并时刻监管技术的应用情况。采用分域式的处理方式来提升网络安全态势感知的效果，与企业整体的管理工作相协调[1]。

3.5 提高信息化技术建设，建立完善的相应管理制度

为推进企业信息化建设，更好地适应社会发展趋势，企业要立足于自身发展现状，建立完善的管理制度与方法，学习现代化的管理思想，将“以人为本”“绿色管理”等优质理念融入企业管理活动中，尊重员工个体差异，培养员工对企业的忠诚度，营造良好的工作氛围，平衡好员工利益与企业利益间的关系，通过创新管理理念来进一步提高企业管理水平。企业要在信息化建设、管理基础上不断调整自身发展目标，将信息化管理理念融入日常活动中，提高管理的科学性和有效性。此外，企业要在信息化实践过程中全面了解安全责任、人员培训制度等问题，优化和调整管理制度与内容，提高信息化建设的灵活性，使管理效果得到保障[2]。

3.6 提高网络信息安全管理

一是构建完善的网络信息管理制度。企业结合自身实际情况，优化现有管理制度中的弊端，通过专家论证等方式，确保相关技术能够得到切实有效的应用。网络安全设备建设差定期化、常态化、确保问题早发现、早处理。在网络环境下应用移动存储设备时必须经过安全检测，对于机密文件的数据传输应采用加密技术。二是进一步完善现有网络信息管理系统。在信息化建设的浪潮中，越来越多的企业构建了网络信息管理系统，并对运营、决策数据分类存储。在存储过程中加强数据安全防御等级，将企业数据信息根据不同的分类原则放置于不同的数据库中，并设置专门密钥，这种存储方式不仅提升了企业的工作效率，还提升了网络数据的安全性，降低了数据外泄的风险。三是提升工作人员责任意识和技能水平。强化网络安全管理员与用户的风险防范意识，一方面企业要落实责任管理制度，将信息安全责任明确到个人，提升相关人员的积极性和责任感，最大程度上避免人为失误出现的安全漏洞。加强对信息安全的实时监控，当出现问题时及时进行纠正；另一方面，在招聘方面严把责任关，确保招聘人员具有扎实的网络安全专业技能。对于已经上岗的工作人员定期开展专业培训，通过专家授课等方式提升工作人员的网络安全防护水平[3]。

4 结语

总之，随着企业信息化建设步伐的加快，企业信息保护面临前所未有的困难和挑战。众所周知，信息安全不仅仅是一个技术问题。安全审计和安全管理是网络信息安全体系的必要组成部分。在使用与安全相关的产品时，必须采取适当的措施来改进系统。公司的信息安全也是一个动态的话题：公司管理层必须定期处理事件和安全要求，及时考虑安全要求的变化并调整安全准则。企业网络安全的现状和问题，然后针对这些网络安全问题提出合适的解决方案，适合大部分企业。当今社会，无论企业规模大小，为了在激烈的市场竞争中生存下来，在企业信息化建设过程中重视网络安全管理是非常重要的。

参考文献

[1] 陈晓阳.企业信息化建设与企业管理创新策略分析[J].老字号品牌营销,2021(6):126–128.

[2] 田影欣.企业信息化建设企业信息化建设问题及对策研究[J].IT经理世界,2021(3):157–159.

[3] 吴振全,于利贤.论如何推进工程咨询企业信息化机制建设[J].科技风,2021(3):166–168.