基于网络信息化的企业保密管理对策研究

Research on Enterprise Confidentiality Management Strategy Based on Network Informatization

汪岑

Cen Wang

中国飞行试验研究院,中国·陕西 西安 710089

Chinese Flight Test Establishment, Xi'an, Shaanxi, 710089, China

【摘　要】在科学技术快速发展的大背景下,信息技术得到了十分广泛的应用。现阶段,在企业的信息化管理过程中,大家大量引入网络信息化管理模式,由于网络环境比较复杂,这就使得信息化管理的安全性成为企业关注的重点。

【Abstract】Under the background of rapid development of science and technology, information technology has been widely used. At present, in the process of information management of enterprises, everyone has introduced a large number of network information management models. Due to the complex network environment, this makes the security of information management a focus of attention of enterprises.

【关键词】网络信息化;企业保密管理;优化对策

【Keywords】network informatization; corporate confidentiality management; optimization of countermeasures

【DOI】https://doi.org/10.26549/gcjsygl.v2i8.1078

1 引言

在社会经济的快速发展中，网络信息技术已广泛应用于人民群众的日常生活和工作中。在全球信息一体化的背景下，大家越来越重视网络环境下的信息安全问题[1]。在企业运行过程中,相关部门通过应用网络信息技术,在一定程度上促进了企业的快速发展,但极易导致企业信息出现泄漏,进而影响企业的正常运行。因此,为了保证网络健康、稳定地运行,相关部门应制定完善的安全管理制度。

2 企业保密管理概述

在企业运营过程中,相关部门应该注重信息的安全性,并实施信息安全管理，其主要目的是避免企业内部的信息受到不利因素的影响，为企业信息系统的安全、稳定运行提供保障。在网络技术发达的背景下,现代化的企业信息安全管理主要是由企业通过相应的科学技术及其软件对信息资料进行管理,为企业信息的真实性、安全性以及完善性提供保障,避免未授权的网络系统受到不利因素或恶意原因的影响而出现信

息破坏、更改或泄露问题。通常情况下，信息安全管理的主要目的是保护企业信息的保密性和安全性，信息安全及其管理联系十分紧密，具有相互促进、相互依赖的作用。在科学技术水平不断提升的时代，很多科学技术得到了一定的发展，比如，云端系统、大数据以及互联网等，逐渐成为企业信息安全管理的工具。因此，在企业的运营过程中，要想实现自身的快速发展，保证信息安全管理的整体质量，相关部门必须注重企业信息安全管理等基础工作，建设信息基础设备和相应的安全保障系统，进而实现企业的可持续发展。与此同时，在社会经济的快速发展中，像云计算、大数据以及互联网等先进技术，推动着IT行业的快速发展。而企业要想实现快速发展，应做好相应的基础工作，完善信息安全保障系统，这样才能够在健康的网络环境中，实现自身的快速发展。除此之外，企业还应该保障内部信息的安全性，深入了解信息安全的重要性，做好信息的保护工作。

3 企业保密管理过程中存在的安全隐患

3.1 网络操作系统的漏洞

通常情况下，在企业运营过程中，普遍存在网络操作系统漏洞现象，且这些漏洞会长期存在，这就使得大量的病毒入侵网络系统。在网络软件设置过程中，为了维护和扩展企业的规模，相关部门往往会设置相应的后门，这些后门往往会对网络安全造成严重的影响，在被不法分子发现后，将严重威胁企业的信息安全，比如，黑客攻击是通过操作系统漏洞而产生的攻击，且黑客攻击往往是由人为造成的恶意攻击，相关人员无法采取相应的措施，对其进行防范，进而严重威胁企业的信息安全，造成难以弥补的后果。

3.2 安全软件设计滞后

在信息技术的快速发展中，计算机网络在企业运营过程中发挥着十分重要的作用。现阶段，计算机技术和互联网技术得到了有效地融合，其不仅能够为企业提供丰富的信息资源，还在很大程度上拓宽了企业获取信息的途径，进而提升了相关工作人员的工作效率，为企业带来了更多的经济效益和社会效益。通常情况下，在企业的运营过程中，往往会涉及拓扑结构的设计以及网络设备选择问题，这就会导致很多病毒和黑客入侵企业内部网络信息系统，严重影响企业信息的安全性。除此之外，相应的病毒查杀软件能有效地解决其中的问题，比如，病毒查杀软件是针对病毒研发的一种“见招拆招”的软件，具有严重的滞后性[2]。因此，在企业的运行过程中，相关技术人员应该注重安全软件的合理应用，这样才能够为自身信息的安全性进行保护，相反，不合理的安全软件设计会为企业信息的安全性带来一定的威胁。除此之外，在安全软件设计不合理或维护不完善的情况下，会有大量的病毒进行入侵，甚至出现系统瘫痪等问题，严重影响企业的顺利运营。

3.3 人为因素造成的安全问题

随着社会经济的快速发展，市场经济体制得到了很大的完善，企业的建设规模在不断扩大，这就使得企业内的竞争日益激烈。而企业在发展过程中，往往只注重自身的经济效益，重视企业的生产运行，无法充分认识到企业信息保护的重要作用，这就使得企业内部缺少相应的机制，严重威胁着企业信息安全保障系统。与此同时，网络是一种新兴的技术，企业缺少对网络技术方面的资金投入，且相关人员的安全意识比较薄弱，相应的安全管理机制不够完善，这就为企业的安全运营带来了威胁，进而使得后期出现一系列的网络安全隐患。

3.4 缺少风险意识和管理意识

通常情况下，企业相关人员普遍缺少相应的风险意识，风险管理技能及其综合素质不够，严重影响着安全信息系统在企业中的有效融合，其主要表现在以下方面：第一，企业相关人员不重视交接文件的安全性，相关部门未安全专业人员进行整理和保管，相应的管理制度和保密措施不够完善，进而导致大量文件的丢失和损坏；第二，在企业运行过程中，员工自拟的重要文件无法得到有效、统一的管理，且极易受多方面因素的影响，导致文件丢失，比如，电脑损坏或丢失、员工中途离职、操作不到位、无意间删除，或在病毒侵入等情况下，都会引发信息安全隐患。

3.5 企业内部缺乏管理

在企业的发展中，由于企业内部缺少统一的管理，极易导致相关部门或工作人员的重要文件丢失或损坏，其主要原因是电脑丢失、员工离职以及操作不当等造成的。同时，在企业的运营过程中，往往会涉及很多文件数据，比如，企业年度、季度和月度的销售总结与分析报告、企业投资与融资报告、财务分析报告、内部会议记录以及商务交流合同与重要文件等，这些文件具有一定的机密性，涉及企业中的财务数据等。与此同时，由于企业内部相关人员不重视重要文件的保护，常常随意将其交付给文职人员进行保管，且缺少相应的管理制度和保

密措施，进而导致相应的文件损坏或丢失。除此之外，很多企业缺少相应的管理意识，无法应用有效、科学的加密措施，处理核心数据和文档，缺少有效的加密技术。通常情况下，工作人员常常使用移动存储、办公室打印、通信工具以及电子邮箱等设备，拷贝电脑中的文件，这就极易引发重要信息的泄漏问题。

4 网络信息化的企业保密管理对策

4.1 建立相应的保护制度

企业内部的人员管理是企业运行过程中的重要问题，为了实现对企业核心数据的有效管理，相关部门必须加强对文档管理人员的管理，这就需要建立完善、合理的保护机制，实现企业核心数据管理工作的顺利进行。与此同时，企业组织内部信息安全保护机制在企业运营过程中占据着十分重要的位置，在企业发展中，相关部门往往需要引进大量新型的设备和技术，还应该构建信息安全保护制度。在企业的发展中，企业内部的攻击比较大，这就需要相关部门建立相应的管理措施，并将其落实到实际工作中，比如，电子文档的起草、处理、传输与搜集、累积和整理、归档并保管以及供给使用的全过程，为文件保护的全程管理提供支持。除此之外，相关部门还应该重视企业信息管理人员和操作人员的管理，通过采取相应的措施，提升相关人员的整体素质，并明确各个人员的岗位职责，及时积累电子档案，并构建合理化的电子档案归档制度，将其落实到位。

4.2 加密技术要改进

为了保障企业信息管理的安全性，相关部门应做好以下工作：首先，加强访问控制。在网络信息化的发展中，相关部门为了避免出现电子文档丢失问题，可以加强对访问的控制。通过控制网络访问和权限，能够强化访问控制，为核心技术的稳定性和安全性提供保障；其次，数据加密。为了实现网内文件、数据、控制信息以及口令传输的安全性，避免电子文档在无法公开的情况下进行公开，相关部门应该重视数据的加密工作，这样能够保障缺少查看权限的人员无法科学地打开文件，或出现文件乱码问题，进而避免出现信息泄露问题；最后，文件备份。为了保证企业信息的安全性，相关部门应该重视文件备份问题。在文件丢失或损毁的情况下，存在文件备份，能够为企业的安全运行提供保障，避免出现大量的损失，从根本上避免文件泄露问题。

4.3 创新企业信息安全技术

网络信息的安全性是网络稳定运行的重要基础。企业要想实现网络信息技术的安全，应从多方面出发，对其进行保护，并将相应的检查机制落实到实际工作中。与此同时，为了适应科学技术的快速发展，相关部门应不断创新企业信息的安全技术，这样才能够实现企业自身的良好发展。为了在技术创新的技术上，提升信息安全技术的整体质量，保证企业自身的经济效益，相关部门应该建立以市场发展为基础的创新机制[3]。除此之外，企业还应该加大对信息安全技术的资金投入，不断创新并改进这一技术，应用相应的制度检查企业信息的实际情况，为企业信息的安全性提供保障。需要注意的是，在企业运营中，相关部门还应该建立相应的应急措施，比如，数据恢复、备份以及销毁等安全预防措施[2]。

4.4 加强人员安全管理质量

人才是信息化管理的执行者，其水平的高低对信息化管理水平存在很大影响。企业应不断提升信息安全管理人员的综合素质，加大人才培养力度，并建立相应的安全组织部门，重视信息人员的认证和审查工作，进而保障企业信息的安全性。企业还应该针对机密信息管理人员，与相关管理人员签订保密协议，为信息的安全提供保障。除此之外，企业应该建立专门的信息安全管理组织机构，不断引进优秀的管理人员，不断提高企业信息的安全水平，实现企业的可持续发展。

5 结语

综上所述，现阶段，企业内部的信息化手段在不断增加，网络信息技术的有效支持下，社会改革在不断深化，在一定程度上推动着企业的快速发展，这就使得人民群众的生活变得更加丰富，为大家的生活和工作提供了很大的便利。因此，为了适应企业现代管理的发展需求，企业要充分认识信息安全管理的重要性，增强对网络和信息系统控制和管理能力，这样才能更有效地促进企业经营和发展[3]。

参考文献

[1]李向华.关于进一步加强和改进信息化条件下保密工作的思考[J].办公室业务,2016(01):71.

[2]李善平.基于网络信息化的企业保密管理对策分析[J].电脑迷,2016(06):16.

[3]葛俊.企业保密工作的隐性漏洞及纠正对策研究[J].中国管理信息化,2017,20(24):88-89.