

## 摘 要

企业的发展和全球化经济的出现促进企业的市场拓展和业务量的大幅提升，同时，互联网的出现及网络技术的不断发展和升级加速网络应用的步伐。伴随着管理信息系统、决策系统和 OA（Office Automation）的推进，企业的办公效率被显著提升，企业对互联网的依赖程度也越发显现出来。今年席卷全球的新冠肺炎疫情，更是把居家办公、停工不停产发挥的淋漓尽致。而网络的安全问题始终是制约网络应用的一大隐患，引起了更多的有识之士和企业的关注和重视。网络安全已经逐步成为衡量、评价企业未来发展速度和提升空间的重要标准之一。

本文通过介绍网络安全的相关理论知识，对 DDRY 公司的网络安全应用现状进行分析，指出除网络安全自身的脆弱性之外，它还存在软件安全漏洞、硬件设施缺陷和人为操作不当等安全隐患，最后，分别从技术层和管理层两个角度提出了企业网络安全系统相应的解决方案。力求从根本上消除各类隐患，构建企业网络安全体系，有效地保障网络安全，为企业的业绩提升和发展壮大服务。

**关键词：**网络安全；隐患；系统

# 1 引言

## 1.1 课题研究背景

随着网络技术和普及，人们的工作和生活都越来越便利，我们的社会正是网络技术的时代。我国的互联网也从无到有、从小到大、由大渐强的发展到现在举世瞩目的成果。世界正在进入一个以信息产业为主导的经济发展时期，为了生存和发展，各行各业的企业也要逐步走向信息化。企业的核心技术、市场资源客户信息等转化成数据并向网络转移。信息化使得企业的工作效率得到提高，而且企业面对市场发展形势走向时的反应能力也能够加强，企业的整体实力也发生了巨变。企业正在使用信息技术来完善自己的信息资源集成系统和业务运营平台。随着计算机等现代办公工具在企业中的普及，工作变得更加便捷，工作效率不断提高。由于网络具有巨大的资源基础，因此企业能够通过整合资源，实现信息共享。但正是由于网络时效性，广泛性和开放性，在网络诞生之初就存在安全风险，网络把我们的生活变的高效和便利，但伴随着迅猛发展的是网络安全问题更加严峻，个人信息与商业数据遭遇泄露与违规利用，关键设施遭到攻击事件时有发生。因此，人们逐步意识到网络安全的重要性，社会也给予重视。根据官方的有关数据统计，有多数企业在利用网络的便捷时，却没有在其计算机中对网络安全进行保护，这是对现在网络安全问题的忽视，对潜在的巨大威胁没有警惕。所以，先要对网络安全有正确的认识，才能有好的警觉性。一般而言，网络安全包括计算机设备安全性、互联网网络信息安全、软件平台安全性。互联网中的一切机器设备都被保护，不容易由于不经意或故意等缘故遭受毁坏、变更、泄漏，可以一切正常运作不中断。如今威胁着网络安全的要素有很多，主要包括以下问题：

计算机病毒的猖獗。计算机病毒存在广，而且极易隐藏在察觉不到的地方慢慢侵蚀着计算机。计算机病毒又能自我复制，传播途径多传播速度快，很难拔除。据相关的数据显示，我国的大部分计算机系统都受到过病毒的干扰，而计算机病毒仍在不断发展更新，变得更加棘手。例如，我们听说过的特洛伊木马，熊猫烧香，脚本病毒，蜗牛病毒等已对我国计算机信息网络安全产生了巨大影响，严重威胁了我们企业的计算机信息安全。计算机病毒的严重危害也迅速引起了人们和社会的重点关注。

黑客的恶意攻击。黑客为了获得想要得到的信息，像某些财政数据、科技成

果甚至是隐私秘闻，一些不法分子可以通过各种攻击手段，例如利用窃取或攻破

获得的密码来明目张胆的窥伺机密文件，在各种网站上植入破坏程序，还有建立假冒网站欺骗用户从而进行窃取或破坏等行为。在电子邮件传输过程中利用非法手段随意截取篡改，来达到自己的目的。现在很多黑客不仅具有较高计算机技术，甚至很多具备一定的知识素养。他们能通过分析人的心理与对应的可能做出的反应来诱导使用者上当。有多数是出于营利目的，他们获得的信息的价值也决定了他们能换取的报酬。还有少数是出于好奇或出于其他目的而进行恶意攻击网络上的用户。这些恶意攻击导致企业和个人信息泄漏，给企业和用户造成巨大损失。据调查，世界各国计算机网侵入的频率已做到 20 秒/次。病毒可以多种方式入侵网络，例如运营商入侵，通常伴随病毒感染系统软件或 U 盘。除了上述的载体入侵之外，计算机入侵的方式是网络入侵。我们每天发送和接收的电子邮件，网页浏览，软件下载等是最不能容忍的，也就是说，出去一次，计算机什么也没做。我发现电子计算机已被黑客入侵。一旦公司的应用系统感染了病毒，它将对公司构成极大的安全风险。如何尽快维护网络信息安全是一个复杂的问题，必须进行多方面的分析。如今，仅通过传统方法来解决网络信息安全问题已不切实际，尤其是在中小型企业中，资金和预算的缺乏为网络信息安全问题带来了隐患。本文还将研究互联网在关键科学领域的现状以及中小企业在应用中的不足，从而开始为中小企业建立网络信息安全的基本构想。与大型企业相比，中小企业在网络安全建设中应遵循完整性，实用性，标准化，可扩展性，易用性和多重保护的基本原则<sup>[2]</sup>。本文通过分析企业网络信息安全的概念和中小型企业网络信息安全的现状，从解决企业网络安全问题入手来研究分析问题和解决方案。<sup>[13]</sup>

## 1.2 课题研究意义

企业的网络安全是关乎企业的信息安全和生存发展的头等大事，如不能及时地处理或彻底解决存在的不完善或漏洞，必将严重制约企业的发展，影响企业的经济效益，严重甚至会波及整个产业链或是行业，甚至造成社会的恐慌和动荡。因此，通过不断探索和研发相关策略和技术，来加强和完善企业网络安全。这对保护企业信息与财产安全，维护社会稳定具有重要作用，对丰富和发展网络安全与防范策略等相关理论和技术都具有一定的理论指导和现实意义。

对于公司而言，在科研成果，信息内容，数据信息等层面都有一些公司关键材料和数据信息。一旦公司关键材料被破坏和损坏，将对公司造成更大的危害。但是，网络信息安全管理体制可以完成其合理的维护。从实际意义出发，不良行为者会根据网络信息安全系统的脆弱性，窃取企事业单位的基本信息，破坏公司

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。

如要下载或阅读全文，请访问：

<https://d.book118.com/798100075136006140>