

# 电子信息技术在企业安全管理中的运用

范青香

杭州休普电子有限公司

DOI: 10.12238/jpm.v6i5.8006

**[摘要]** 电子信息技术的发展,为企业安全管理提供了很大的便利。但是随之产生的安全性问题确实是不容忽视的,本文首先介绍电子信息技术在企业安全管理中发挥的重要作用,分析其中存在的安全性问题,最后针对性提出解决性的措施。企业管理者需要从防范意识上、技术层面上、管理层面上,多管齐下,建立适合自身发展情况的信息安全管理方案,维护企业信息安全,以助力企业获得更好发展。

**[关键词]** 电子信息技术;企业;安全管理;应用探究

## Application of electronic information technology in enterprise safety management

Fan Qingxiang

Hangzhou Xiupu Electronic Technology Co., LTD.

**[Abstract]** The development of electronic information technology has greatly facilitated enterprise security management. However, the security issues that arise are indeed not to be overlooked. This paper first introduces the significant role of electronic information technology in enterprise security management, analyzes the existing security problems, and finally proposes targeted solutions. Enterprise managers need to adopt a multi-pronged approach from awareness of prevention, technical aspects, and management levels, to establish an information security management plan suitable for their own development, safeguarding enterprise information security to support better corporate growth.

**[Key words]** electronic information technology; enterprise; security management; application exploration

电子信息技术在企业生产生活中的应用日益广泛,虽然提高了工作效率,但也存在着一定的安全风险。企业在实施信息共享和下载管理过程中,经常受到计算机病毒的攻击,这些攻击不仅给企业带来了巨大的经济损失,也给公司的未来发展带来了巨大的影响。因此,企业管理者应当加强自身的安全意识,运用电子科学技术对网络安全存在的问题进行处理,并结合企业的发展状况,制定一系列的信息安全管理方案。唯有如此,才能确保安全生产,确保企业的经济效益。

### 一、浅谈电子信息技术对企业安全管理工作的重要意义

电子信息技术是指利用计算机等现代科学技术对电子信

息进行控制与处理的一门学科。现在,电子信息技术已经渗透到了我们的生活的各个方面,例如,电话交换局如何处理各类电话信号,手机如何传输声音和图像,周围的网络如何传输,就连信息化的军事通信,都离不开电子信息的应用技术。我们需掌握电子信息技术的基础知识,并把先进的技术应用于新产品的研究与开发。当今的市场是一个信息大爆炸的市场,谁能够及时地获得资讯,占据最多的资讯,才能掌握市场的最新动向,从而对市场的决策与运作做出正确的判断。而信息技术的加工、储存与接收等工作,则以电子化的方式进行。因此,建立一个完善的企业信息化体系是非常必要的。运用电子信息技

术, 对企业发展所需要的各种信息资源进行开发与使用, 尤其是国内外市场以及它们的变化情况, 从而提升企业在国内外市场环境中的竞争力, 实现企业在世界范围内的竞争中获得并维持自己的优势。

## 二、企业信息安全管理的现状

### (一) 电子信息安全管理漏洞

虽然目前电子信息技术正处在一个比较好的发展时期, 但也有些技术还处在发展的初期, 在实际的应用上并没有得到很好的完善, 所以, 在企业的经营和管理过程中, 必然会出现一定程度的信息安全风险。在电子与资讯科技飞速发展的今天, 电子信息产业的竞争日趋激烈, 一些企业, 会采取一些不正当的手段, 比如盗取对方的数据, 从而造成企业数据的泄露。在计算机技术飞速发展的今天, 如果不能对其进行有效地修复和处理, 就有可能被犯罪分子有机可乘, 从而威胁到计算机系统的安全。目前, 在企业信息化过程中, 信息安全是一个非常重要的问题, 也是一个迫切需要解决的问题。

### (二) 企业信息安全防范意识弱

对大部分企业来说, 利用计算机和网络技术来处理各种工作已经成为一种普遍现象。但在这其中, 仍有一个非常重要的问题存在——员工对安全生产知识的欠缺。虽然大多数企业的安全管理已经取得了长足的进步, 但是在实践过程中, 依然会因为基层员工的疏忽大意而被忽略。这是因为企业在开展内部的安全管理会议和培训工作时, 不能具体到每个人, 而是要通过部门领导的统一指导, 将安全管理需要关注的各个方面传达给大家。各部门负责人在传达具体要求时, 难免会有疏漏或出错, 况且, 公司的内部管理体系中, 并没有针对安全管理方面的过失进行处罚, 很多人会认为, 这件事与自己毫无关系。即便在企业的生产运作中, 存在着某些信息方面的漏洞, 但是由于员工的意识、专业水平不足等因素, 常常会导致安全管理的基本条件不健全, 最终导致不断增加的安全隐患, 给企业带来无法弥补的经济损失。

### (三) 缺乏完善的防火墙体系

计算机网络的应用已经深入到了员工的工作和生活中, 互联网的发展给我们带来了便利, 但也给木马病毒留下了可乘之机。计算机使用中最大的安全隐患就是病毒感染和恶意攻击,

这给企业的网络安全带来了巨大的隐患。如果计算机中毒, 它会让计算机的运转变得非常缓慢, 从而严重地影响工作效率。大多数的黑客都是别有用心, 他们在计算机中安装了病毒, 然后远程操控计算机, 获得了公司的资料, 给公司的经济带来了很大的负面影响, 因此, 在企业的安全管理工作中, 应该采取一些行之有效的方法, 将这一风险降到最低。

## 三、电子信息技术在企业安全管理中的具体应用分析

### (一) 增强信息安全的防范意识

在当今科技高速发展的时代, 安全管理已经越来越成为一个不可或缺的话题, 对于企业的生产经营也越来越重要。然而, 由于缺少有效的预防手段, 并且缺少一套行之有效的监督机制, 在企业的安全管理中, 信息化的应用还面临着许多问题和挑战。为了解决这一问题, 需要制定一套完善的操作规范。这套标准不仅要细化信息安全的各项措施, 还要让大家切实贯彻执行, 从而形成自上而下的执行力。

在新企业成立之初, 企业应加大对员工的培训和指导, 使其认识到, 信息安全不仅是公司领导的责任, 也是每一位员工的责任。与此同时, 加强对 IT 管理人员的培训与引导, 为其提供更多的工作机会, 促进其职业发展。只有把安全管理列为企业的一项重要工作, 才能更好地协调、控制企业的信息、数据, 避免因员工的失误而造成泄露。通过构建专业化、针对性强的信息化管理体系, 使企业的基础管理水平得到了进一步的提高, 同时也能提高企业员工的工作效率和反应能力。同时, 如果管理者能够在企业发展目标和信息管理的要求上取得一致, 并且能够严格地贯彻实施, 那么他们就能够充分地运用自己的领导才能和影响, 为公司的日常经营做出一个好的榜样。从上到下, 对工作进行有效地导向与激励, 既可以有效地防范信息安全风险, 又可以提高信息数据的应用可靠性与稳定性。

### (二) 构建安全网络平台

现代网络技术的飞速发展, 给企业带来了难以掌控的网络环境, 同时也会造成企业内部的信息资源的损失。为了应对这一挑战, 企业必须加大防火墙的投入, 并提高防火墙的性能。通过对防火墙的有效应用, 可以极大地提高对病毒和黑客攻击的抵御能力。它的使用不能仅仅局限于防火墙的基础配置, 还应延伸至保护软件的研发与应用, 以达到整个系统的协调与

安全。同时,根据企业自身的发展需要,需要通过建立一个网络化的管理系统,进而搭建一个安全管理平台。这其中既有研发的软件,也有安全芯片的应用。这种管理方式能够使企业内部的网络平台得到最大程度地发挥,在信息管理方面,它的安全性也会得到进一步的提高,从而更好地保障企业信息安全,为企业的管理提供了更可靠的技术途径。在现代企业的管理实践中,员工身份和职责是一个不可忽视的要素。随着组织结构日益复杂,企业内部员工必须清晰地认识到他们所处的职务等级及其相应的权限范围。这种对个人角色的明确划分,是确保内部信息安全、防止数据泄露的关键策略之一。

具体来说,企业会根据每个员工的职务性质和职务等级,赋予其不同的信息访问权限。这意味着他们能够浏览或获取哪些类型的文件,而这些文件可能包含了公司的商业秘密或是敏感的内部数据。通过对不同职务性质和等级的员工设置不同的权限,可以有效地保护那些高层管理者所关注的保密资料,使之不会轻易被非法人士获取或因保管不当而丢失。此外,实行严格的分层信息管理制度,还旨在确保每位员工的工作权限得到合理分配。在这个框架下,员工只能访问与自己直接相关的信息和资料,而无关的内容将不能被获取。这样一来,不仅可以有效防止机密信息的外泄,还能提升整个团队的工作效率和响应速度。因为当员工只接触到他们应该处理的资料时,他们就能更加专注于手头的工作,减少不必要的时间浪费。

### (三) 精加大资金投入, 强化硬件设施

对于企业单位而言,加强信息安全管理不仅仅是一项技术任务,更是对整个企业文化和运营模式的全面升级。要实现这一目标,企业必须从高层领导做起,他们的理念将直接影响到整个组织的安全态势。当领导者们开始认识并重视信息安全的重要性时,接下来的工作就是让这种意识在整个企业中传播开来,逐渐渗透到每一个员工的心中。这样,企业就能构建起一种自上而下、全员参与的信息安全管理体系,从而形成一个坚不可摧的内部防线。对于企业单位而言,加强信息安全管理不仅仅是一项技术任务,更是对整个企业文化和运营模式的全面升级。要实现这一目标,企业必须从高层领导做起,他们的理念将直接影响到整个组织的安全态势。当领导者们开始认识并

重视信息安全的重要性时,接下来的工作就是让这种意识在整个企业中传播开来,逐渐渗透到每一个员工的心中。这样,企业就能构建起一种自上而下、全员参与的信息安全管理体系,从而形成一个坚不可摧的内部防线。

面对市面上种类繁多的防护软件和工具,企业高层管理者应当主动寻求专业意见,聘请具有专业背景的网络安全专家来负责软件的测试和评估。通过这样的方式,企业可以筛选出真正符合其需求和条件的产品,并确保这些软件能够有效地保护企业内部的信息资产免受各种威胁。同时,设立专门负责电子信息技术部门是确保企业信息和数据安全的另一个关键步骤。这个部门应该拥有一支专业的团队,专注于研究和实施先进的技术解决方案,以应对不断变化的信息安全挑战。通过这种专业化的管理,企业能够更加高效地管理和监控其信息系统,确保数据的完整性、保密性和可用性。

### 总结

总而言之,电子信息技术已经渗透到了当今社会的各个领域,尤其是在现代工业领域,它的发展给企业的安全管理提供了更加方便和有效的解决办法,但我们不能仅仅看到它的积极一面,也要看到它的消极影响。相关工作人员要加大对先进技术的应用研究,同时也要提高员工的意识,在公司的各个层面上都要对电子信息的安全管理给予足够的关注,只有这样,他们才能在日常的工作中,合理地运用各种技术手段,保证信息共享和浏览的安全,推动公司的安全、高效地发展。

### [参考文献]

- [1]王兴毅.电子信息技术在安全保障管理中的应用[J].数字通信世界.2024(1)
- [2]张琛.电子信息技术在企业安全管理中的运用[J].中国市场,2019(21)
- [3]赵岩.电子信息技术在企业安全管理中的运用[J].科学与财富,2020

作者简介:范青香;出生年月,1977年3月27日,女,民族:汉,籍贯:山西,职务:副总经理,学历:硕士,研究方向:企业管理。