电子商务网络安全问题现状与防范对策

杨涵羽
（浙江省机电技师学院，浙江 义乌 322000）

摘要：互联网时代电子商务为生产、生活带来更多便利，为电子商务活动提供十分广阔的发展空间，同时也给电子商务信息安全防范提出更高要求。现阶段的电子商务活动面临较多的网络安全问题，如病毒入侵、信息泄露等。所以如何借助网络空间、资源共享和服务拓展确保电子商务活动顺利进行、防范不良因素，成为众多电子商务企业关注内容。本文就电子商务网络安全问题现状与防范进行研究，并对此提出相应看法。

关键词：电子商务；网络安全问题；现状与防范；研究

进入新时期以来，电子商务成为一种全新的商业模式，其可以借助网络资源的优势传输各类商业信息，进而在很大程度上简化商品交易流程，实现了商务活动的电子化、数字化发展。电子商务的兴起在很大程度上丰富了群众的生活，同时也给一些不法分子提供可可乘之机，其中窃取客户信息、盗用消费者账号的情况较为严重。出现相关问题的重要因素在于电子商务中有大量的客户交流信息，且用户购买记录可随意查询，这使得电子商务活动的信息保密工作面临较大挑战，且一些企业并未重视电子商务网络安全问题，使得安全问题频发。针对这一情况，在开展电子商务活动的同时，企业需要顺应时代发展重视电子商务网络安全问题，通过分析发展现状落实相应的改善措施，从而实现可持续化发展。

一、电子商务网络安全管理的必要性

（一）提升电子商务网络安全管理工作效果

进入新时期以来，更多的电商企业在发展中开始关注网络安全问题，在实际发展中开展针对网络安全引入诸如智能化管理手段。学习、推理能力十分优秀，是全新技术手段的重要应用价值，便于电商企业管理人员对各项信息进行有效处理。以往的电商企业网络安全防御系统相对单一，且多数系统不够智能化，这并不利于企业有效发展。依托人工智能技术的学习和推理能力，很多企业开始引入此项技术，在网络安全防御与管理中，人工智能技术可以对计算机系统中正在发生或已经发生过的安全风险进行分析、学习，及时找出互联网庞大数据信息之间的关联性，随后通过对这些信息进行归纳总结、判断推理，高效率地从中获取网络安全工作的可靠性数据，帮助管理者提出科学的网络安全防御方案，从而提升信息处理效率，在最大程度上避免电商网络安全问题的出现。

（二）规范化电子商务工作流程

实际上，目前很多电商活动中合同签订意识借助网络完成的，而企业不断优化电商网络平台，能够确保交易时间、送货方式、付款方式、送货地址等流程的稳定运行。在这一过程中若出现泄露签订信息的情况，会对企业的有效竞争、保护用户隐私等造成一定影响，给一些不法分子提供可乘之机。因此，电商企业重视网络安全问题，能够确保各类交易信息、客户信息的保密性，使企业与客户均有信息安全保障。

此外，良好的网络平台能够防范商品交换与结算阶段。这一阶段频发类似的电商网络安全问题，而企业对此引入全新技术手段、全新方式是十分关键的，如淘宝网、易趣网等运用的支付宝软件就是一种很好的防范发布虚假消息诱骗消费者的手段。此外，引入一定的保险机制，加大对网络安全信息防范技术的投入，引进相关专业的技术人才为商品的交换与结算阶段营造坚实的安全壁垒，切实提高电商平台的安全性与稳定性。

二、电子商务网络安全问题现状

（一）电商企业工作人员网络安全防范能力不足

在当前科学技术以及互联网飞速发展的背景下，生活以及生产中出现的网络病毒类型、数量等不断增多，且一些黑客技术能力也在不断创新，为了在最大程度上避免出现安全类问题，则需要相关部门适当加大网络监管和监督路阻，并能够结合实际需求做好网络异常情况处理，针对不同问题制定有效解决方案。但是在实际落实过程中，电商企业会受到不同因素影响以及限制，总体来看目前很多电商企业工作人员综合素养较差，相关监测能力并未达标，同时很多单位的网络监管以及监测能力相对较差，并未从多方面入手开展网络管理监管等。这些因素的共同制约使得技术部门、企业等单位难以及时发现网络安全中存在的问题和隐患，以至于出现病毒入侵得不到及时处理，这在很大程度上影响了企业、个人发展，甚至会导致企业产生相应的经济损失，

（二）电商平台的防范性较差

现阶段，互联网技术、信息化平台等成为生活以及生产的有力推手。对新时期下的电商企业来讲，其为了进一步提升经济效益，互联网也在不断发展以及更新，且为了最大化其利用价值，电商企业的网络安全管理技术、手段等有必要与时俱进一同变化。不过结合部分企业和单位实际情况进行分析，一些单位在发展中并未有效迎合互联网技术变化，同时也并未发展相应技术，使管理能力与实际需求不足。同时，近年来国内有一些电商企业投入大量资源研发信息管理加密技术，但起步晚、经验少，所以遇到了很多坎坷与挫折，导致电商企业既定的发展目标难以实现。

（四）网络病毒给电子商务造成的损失继续增加

结合相关的调查资料进行分析，当前阶段电子商务交易中，浏览器信息被篡改、系统使用受限等，均会给电子商务企业造成不良影响。当前，多数企业的管理系统难以在统一时间内完成购买，且很多设备后期管理工作相对烦琐，使得企业的安全管理对策难以统一落实，这在一定程度上增加了电子商务网络安全管理难度；一些企业缺少相应的网络使用和管理制度，这一情况的出现使得企业难以有效对网络用户行为进行监管，很容易出现类似的网络安全问题。

三、电子商务网络安全问题防范对策

（一）提升技术人员网络安全意识

在电商网络安全管理过程中，为了给员工、客户等带来良好的电子商务体验，避免出现网络安全问题，相关单位在发展中应

重视技术人员、安全管理人员综合能力提升，管理人员能够结合电子商务运营平台实际情况以及需求对网络资源进行有效配置，以此来确保网络平台能够处于正常状态。为了实现这一发展目标，笔者认为企业在发展中可从以下几点入手提升技术人员综合能力：首先，企业需要转变发展理念，意识到电子商务网络安全对企业综合发展的影响。计算机网络管理人员需立足实际，结合企业绩效管理体系和人员素质提升体系，引导技术人员积极参与各类培训，使其掌握全新的技术以及方法，并将这些内容落实于网络安全管理过程，及时解决当前管理工作中存在的难点问题；同时企业也需同时出台相应的奖励机制，鼓励相关的管理人员积极参与培训过程。其次，为了确保技术人员综合能力可满足现阶段高校网络安全管理实际需求，管理人员也需要进一步完善相应的管理方案。具体来讲，企业管理人员可以发放调研问卷，及时、精准地掌握员工对内部培训体系和绩效体系存在的疑惑以及建议，并汲取其中有价值的内容将制度进一步完善，避免实际培训工作出现偏差。第三，企业选择有针对性并符合员工实际需求的培训方法，企业需围绕电子商务网络安全管理内涵、员工实际需求，结合其差异性可以落实分层培训法，确保员工整体能力和素养的提升，从而进一步提升电子商务平台的安全性与稳定性，为后续活动的顺利开展做好充分保障。

（二）搭建安全防范系统

安全防范系统能够进一步提升电商平台的稳定性，确保交易活动能顺利进行，且能够避免用户、企业信息泄露。第一，针对日常维护工作，技术人员需要及时查看监控软件，围绕其信息反馈情况了解网络现状；对路由器、防火墙等落实日志监控，若发现其中存在安全类问题，则需要及时解决，以防出现计算机病毒；制定完善的物理安全防护措施，降低人为、自然灾害等对网络安全的影响，如企业可进行用户验证码的设置，对其使用权限做出合理约束，避免出现越权操作情况。第二，企业搭建并完善安全防护系统。一方面，企业需要完善内部系统。在实际发展过程中，高校计算机管理部门需要借助计算机中的大数据系统，建立并完善内部运行程序，并适当优化不同领域中数据系统之间所建立的网络数据资源管理库，如计算机网路和程序中应用计算机大数据的信息数据建立虚拟信息链，信息链在计算机网络数据资源运行中，逐步建立新的数据资源保护链，实现资源贯通。另一方面，建立外部保护系统。第三，重视文件备份以及资源管理。针对可能出现的突发事件，资源管理平台能够在最大程度上避免出现数据文件丢失情况。

（三）持续完善内部的安全管理制度

完善的安全管理制度，同样是确保电子商务网络安全的重要保障，对此相关的电商企业应逐渐建立并完善安全管理制度，避免后续工作出现偏差。第一，企业明确网络安全管理工作制度。这一制度的落实有利于电子商务网络安全管理工作进一步规范行为，确保制度具体化并贯穿于企业电商网络安全管理各个环节，切实构建新时期下的网络安全管理和防范体系。第二，系统操作安全管理制度。企业在发展中需积极顺应时代发展，建立并落实必要的安全防范体系、系统，这样能够确保网络安全性以及可靠性，切实提升电商网络安全平台的稳定性。第三，风险调控体系。风险调控系统能够降低安全事件发生概率，相关技术的主要工作原理在于将大量的处理信息分为内外两个管理系统，其中内部管理系统的安全要求较高，其重要部分的数据都可以被纳入到内部管理系统中。同样的，若立足全新层次进行分析，防范系统的不断完善以及升级，也会不可避免地造成网络病毒、黑客水平升级，使得网络安全存在大量隐患，同时企业也要将这一体系建设视为长期工作，以此来应对突发的电商网络安全类问题。

（四）积极引入多重网络技术

1. 运用密码技术，强化通信安全

企业需要重视数字证书的应用和引入，从而为电商平台信息网络中不同业务的应用提供真实信息，确保信息完整性。此外，在业务系统中也要建立长期且有效的责任机制、信任管理机制，例如现阶段需要强化身份认证、数据加密等工作，具体是对电商中不同类型的敏感数据进行加密处理，同时在数据传输过程中也要做到加密处理，这样能够防止出现数据被窃取的情况。新时期下电子商务信息交换过程中的不同信息，需要借助身份认证的方式确认其合法性，随后明确用户个人数据及其相应权限；针对多个认证实体的认证，则需要企业引入相应的 PKI 技术，通过第三方（CA）颁发的数字证书数字签名来确认彼此身份；对社会管理部门来讲，为了在最大程度上杜绝电商平台网络安全问题的出现，安全产品的应用应建立在国内自主研发的产品基础上，可参考先进地区的相关技术，但不能完全照搬，以提高我国信息企业的技术和管理水平，促进我国电子商务安全建设与发展。

2. 加强技术管理

第一，围绕相关标准严格控制相关部门对网络资源的使用。基于电子商务平台，除去有特殊需求而不能轻易放开的共享目录，针对经常交换信息要求的用户，在这一过程中需要确保信息加密，相关人员在输入正确密码后方访问相关数据。第二，针对涉及机密信息的用户主机，使用人员在应用过程中需尽可能减少开放一些不常用的网络服务，并关闭一些端口，且需要对数据库中的数据进行备份处理。第三，在最大程度上保障媒体安全性。要防止系统信息在物理空间上的扩散；为了防止系统中的信息在物理空间上的扩散，可引入相应的电磁屏蔽技术，减少或干扰扩散出去的空间信号，从而确保企业电子商务平台的安全性。

四、结语

综上所述，在新时期下电商企业重视网络安全管理，能够进一步改善当前网络管理现状，确保企业稳定发展。因此，企业管理人员需要顺应时代发展，深入分析当前电商网络安全管理角度存在的问题，随后从提升人员综合能力、优化管理体系、积极引入全新的技术手段入手，构建新时期下的电商网络管理格局，避免出现类似的网络安全问题。

参考文献：

[1] 罗志坚，董满 . 浅谈电子商务网络安全问题现状及防范措施 [J]. 石河子科技，2022（01）：36-37.

[2] 杨红霞 . 电子商务网络安全问题现状及防范措施 [J]. 信息与电脑（理论版），2018（15）：217-220.

[3] 李亚文 . 电子商务背景下自动识别系统中的网络安全问题及措施 [J]. 信息与电脑（理论版），2018（13）：226-227.

[4] 张金旺 . 电子商务网络安全问题及对策 [J]. 教育信息技术，2018（Z1）：94-96.