数字经济产业发展中网络安全面临的形势、存在问题及对策研究

杨志文

江西服装学院大数据学院，江西南昌，330201；

摘要：数字经济产业蓬勃发展，[1]已成为推动经济增长与变革的核心力量，然而，网络安全问题如影随形，严重制约其稳健前行。目前，全球网络空间对抗和实战化加剧，数据与信息安全风险攀升，数字经济还衍生出新型经济社会安全风险，网络安全威胁呈现常态化、复杂化、组织化与高级化趋势，并向多领域传导渗透。在发展过程中，存在着新技术新业态安全防护能力弱、网络安全问题跨平台跨业务、攻击面扩大、线上线下融合致安全需重新定义、威胁不断加剧以及人才资源不足等问题。为应对这些挑战，应提升网络安全防护、数据安全保障及风险研判能力；积极开展国际合作，参与规则制定；加强顶层规划设计，强化基础设施防护；完善数据相关规则，促进数据合理流动，以此筑牢数字经济产业发展的网络安全屏障，推动数字经济高质量发展。

关键词：数字经济产业；网络安全；问题及对策

DOI：10.64216/3080-1486.25.03.048

1 数字经济产业与网络安全的关联

1.1 数字经济产业的发展态势

近年来，数字经济产业展现出强劲的发展势头，成为推动全球经济增长的核心力量。在规模上，其体量持续快速扩张。据权威数据显示，过去数年，全球数字经济规模以每年两位数的速度增长，在各国 GDP 中的占比不断攀升。

从发展趋势来看，技术创新驱动特征显著。[2]云计算、大数据、人工智能、区块链等前沿技术不断迭代升级，加速向各行业渗透融合。此外，数字经济产业的应用场景日益丰富，从日常的线上购物、移动支付，拓展到智慧城市、智慧医疗等领域。同时，随着 5G 网络的普及，将进一步催生更多创新业态，为数字经济产业的发展注入新的活力，持续改变着人们的生活和生产方式。

1.2 网络安全对数字经济产业发展的关键作用

1.2.1 保障数据安全与隐私

在数字经济产业中，数据已然成为核心资产，保障数据安全与隐私至关重要。

数据安全关乎数字经济产业的生存与发展。数字经济产业运营积累的海量用户数据、商业机密等，一旦泄露，可能引发严重后果。

保护用户隐私是数字经济健康发展的基石，为保障数据安全与隐私，数字经济产业需部署先进的加密技术，防止数据传输与存储过程中被窃取；建立严格的访问权限管理机制，确保只有授权人员能接触敏感数据；同时，加强员工数据安全意识培训，避免因人为疏忽造成数据泄露事件 。

2 数字经济产业发展中数字经济产业网络安全面临的形势

2.1 数据泄露风险高

数字经济产业在日常运营中积累了海量数据[3]，涵盖客户信息、设计图纸、销售数据等。客户信息包含姓名、联系方式、购买偏好等，一旦泄露，不仅会损害客户权益，引发信任危机，还可能导致企业面临法律诉讼。而且，由于数字经济产业业务广泛，数据存储和传输环节众多，增加了数据被攻击和泄露的风险点。

2.2 网络攻击手段多样

黑客攻击手段层出不穷，对数字经济产业构成严重威胁。常见的如 DDoS 攻击，恶意软件攻击也较为常见，如病毒、木马等，可能会潜入企业内部系统，窃取敏感数据或破坏系统功能。网络钓鱼更是防不胜防，黑客通过发送伪装成合法机构的邮件，诱使员工点击链接或提供敏感信息，从而获取企业网络访问权限。

2.3 供应链安全隐患

数字经济产业的供应链涉及众多供产业。[4]在数字

化供应链中，任何一个环节的网络安全防护薄弱，都可能成为黑客攻击的入口，进而影响整个供应链的稳定运行。物流环节信息泄露，则可能导致货物运输轨迹被监控，增加货物丢失或被盗风险。

2.4 安全意识与投入不足

部分数字经济产业对网络安全重视程度不够，员工网络安全意识淡薄，容易在不经意间成为网络攻击的突破口，如随意点击不明链接、使用弱密码等。同时，一些企业为控制成本，在网络安全防护方面投入较少，缺乏先进的安全防护设备和专业的安全团队，难以应对日益复杂的网络安全威胁。

3 数字经济产业发展中数字经济产业网络安全存在的问题

在数字经济浪潮的推动下，数字经济产业数字化转型进程不断加快，线上业务拓展、供应链数字化协同等都依赖网络信息技术。然而，当前数字经济产业在网络安全方面存在诸多问题，阻碍了企业的稳健发展。

3.1 安全管理体系不完善

许多数字经济产业缺乏健全的网络安全管理体系。[5]一方面，没有制定明确的网络安全策略和规范，员工在日常操作中无章可循，另一方面，应急响应机制缺失或不完善，当遭遇网络安全事件时，企业无法迅速采取有效的应对措施，导致损失扩大。

3.2 技术防护能力薄弱

从防护技术层面来看，数字经济产业普遍存在短板。部分企业使用的防火墙等安全设备老旧，无法抵御新型网络攻击。以一些高级持续性威胁（APT）为例，传统防火墙难以检测到其隐蔽的渗透攻击行为。同时，加密技术应用不足，在数据传输和存储过程中，大量敏感数据未进行有效加密，一旦被截获，就容易被窃取和篡改。此外，漏洞管理不善，企业未能及时发现和修复系统中的安全漏洞，黑客可利用这些漏洞轻易入侵企业网络，获取关键数据。

3.3 人员安全意识淡薄

员工是企业网络安全的第一道防线，但数字经济产业员工的网络安全意识普遍淡薄[6]。不少员工随意在办公设备上使用来路不明的移动存储设备，这些设备可能携带病毒或恶意软件，一旦接入企业网络，就会导致病毒传播和数据泄露。在邮件处理方面，员工缺乏对钓鱼邮件的识别能力，容易被伪装成合作伙伴或上级领导的邮件所迷惑，点击其中的恶意链接或下载附件，从而使企业网络遭受攻击。而且，员工对密码安全重视不够，设置简单易猜的密码，或者多个账号使用同一密码，增加了账号被盗用的风险。

3.4 供应链安全协同难

数字经济产业的供应链复杂，涉及众多上下游企业。在数字化供应链中，各环节之间的网络安全协同存在困难。[6]企业与供应商、物流商等之间缺乏有效的安全信息共享机制，一方出现安全问题时，难以及时通知其他方做好防范。同时，不同企业的安全标准和防护水平参差不齐，防护薄弱的企业容易成为供应链安全的短板，为黑客提供攻击入口。

3.5 安全人才短缺

专业的网络安全人才匮乏是数字经济产业面临的又一难题。与互联网等科技企业相比，数字经济产业对网络安全人才的吸引力不足，导致企业内部安全团队规模小、技术水平有限。安全人员缺乏应对复杂网络安全问题的能力，在面对新型网络攻击时，往往束手无策。

4 数字经济产业发展中数字经济产业应对网络安全问题的措施

在数字经济蓬勃发展的时代，数字经济产业数字化转型进程不断加速，网络安全已成为企业稳健发展的关键因素。面对前文所述的诸多网络安全问题，数字经济产业需采取一系列行之有效的措施加以应对。

4.1 完善安全管理体系

建立健全网络安全管理体系是数字经济产业的首要任务。首先，制定详尽的网络安全策略与规范，明确各部门、各岗位在网络安全方面的职责和权限。其次，完善应急响应机制，制定详细的应急处置预案。定期组织应急演练，确保在遭遇网络攻击或数据泄露等安全事件时，数字经济产业能够迅速做出反应，及时切断风险源头，通知受影响的客户，降低损失并维护企业声誉。同时，建立安全审计制度，对企业网络活动进行实时监控和定期审计，以便及时发现潜在的安全隐患。

4.2 提升技术防护能力

加大在网络安全技术方面的投入，提升技术防护能力至关重要。数字经济产业应及时更新防火墙、入侵检测系统（IDS）和入侵防御系统（IPS）等安全设备，采用先进的人工智能和机器学习技术，增强对新型网络攻击的检测和防御能力。建立漏洞管理平台，定期对企业内部系统进行漏洞扫描，及时发现并修复安全漏洞。同时，关注软件供应商发布的安全补丁，及时进行更新，

防止黑客利用已知漏洞进行攻击。

4.3 强化人员安全意识培训

人员是网络安全的核心因素，强化员工的安全意识培训刻不容缓。定期组织网络安全培训课程，向员工普及网络安全基础知识，包括如何识别钓鱼邮件、防范恶意软件、设置强密码等。通过实际案例分析，让员工深刻认识到网络安全事故的严重性和危害性。开展网络安全意识宣传活动，建立员工安全行为考核机制，对遵守网络安全规范的员工给予奖励，对违反规定的员工进行惩罚，激励员工自觉遵守网络安全规则。

4.4 加强供应链安全协同

数字经济产业应重视供应链网络安全，加强与上下游企业的协同合作。建立供应链安全信息共享平台，实现各企业之间安全信息的实时共享。当一方发现安全威胁时，能够及时通知其他企业采取相应的防范措施。[7]共同制定供应链网络安全标准，要求所有参与企业遵循统一的安全规范，提高整个供应链的安全防护水平。对数字经济产业进行定期的安全评估和审核，确保其具备足够的网络安全防护能力。

4.5 引进和培养专业安全人才

为解决网络安全人才短缺问题，数字经济产业应积极引进和培养专业人才。一方面，提高企业对网络安全人才的吸引力，提供具有竞争力的薪酬待遇和良好的职业发展空间，吸引外部优秀的网络安全人才加入。另一方面，加强企业内部安全人才的培养，建立完善的培训体系，定期组织内部安全人员参加专业培训课程和行业研讨会，不断更新其知识和技能。鼓励安全人员参加相关的认证考试，提升其专业水平。此外，还可以与高校和专业培训机构合作，开展定制化的人才培养项目，为企业定向培养网络安全专业人才。

5 结论与展望

数字经济服装产业在蓬勃发展的同时，网络安全问题不容忽视。从当前形势来看，网络攻击手段日益复杂多样，攻击目标不断扩大，涵盖了各个行业领域，这对数字经济产业的稳定发展构成了严重威胁。

在存在问题方面，网络安全意识淡薄、技术与人才短缺[8]、安全管理制度不完善以及新兴技术带来的安全挑战等，都是当前亟待解决的难题。这些问题使得数字经济产业在面对网络攻击时，往往处于被动防御状态，难以有效保障数据安全和业务的连续性。

针对这些问题，需强化网络安全意识教育，[9]加大安全投入与技术创新，加强人才培养与引进，完善安全管理制度与流程等。通过这些措施，逐步构建起全方位、多层次的网络安全防护体系。

展望未来，随着数字经济的持续发展，网络安全将愈发重要。一方面，技术创新将成为提升网络安全防护能力的关键。另一方面，行业间的合作与交流也将不断加强，通过共享安全威胁情报、联合开展安全研究等方式，共同应对日益严峻的网络安全挑战。只有全社会共同努力，持续完善网络安全防护体系，才能为数字经济产业的健康发展营造一个安全、稳定的环境。

参考文献

[1]张立斌.数字经济概论[M].北京：科学出版社，2020 年.
[2]中国市场调研网报告，网络安全战略与方法发展现状、趋势及展望[R]，2025 年.
[3]联合国贸易发展委员会.2024 年数字经济报告（概述）[R]（2024 年）.
[4]余晓晖.2024 全球数字经济白皮书.[R]央广网，2024 年.
[5]金融时报.守好数字金融安全底线[R].中国金融新闻网，2025 年.
[6]陈月华、陈发强.密切关注数字安全发展态势保障数字经济高质量发展[J].保密科学技术，2023.
[7]张悦、刘辉.数字经济产业供应链网络安全协同机制构建研究[J].物流与供应链管理，2022.
[8]邬贺铨.数字经济发展的关键问题与对策[J].管理世界，(3),1-15.2024.
[9]王强、李明.数字经济下数字经济产业网络安全风险及防范策略研究[J].经济管理研究，30(4),25-36.2023.

作者信息：杨志文，男，1966 年 12 月生，汉族，籍贯：江西南昌，学历：硕士，职称：教授，研究方向：计算机技术综合应用

基金课题:2025 年江西省计算机用户协会重大课题《数字经济产业发展中网络安全面临的形势、存在的问题及对策研究》（JXCUA-KTLX-2）