DOI: 10.16538/j.cnki.fem.20241024.204

网络安全风险与ESG投资
——基于声誉保险机制的解释

张才师, 刘 益
（上海交通大学 安泰经济与管理学院, 上海 200030）

摘 要: 尽管网络安全已成为企业不容忽视的风险源，但目前对企业如何有效防范和应对网络安全风险的研究仍相对有限。基于ESG投资的声誉保险机制，以中国A股2010—2022年上市公司为研究对象，实证检验了网络安全风险对企业ESG投资的影响效应与影响机制。研究发现，网络安全风险越高的企业，越有可能增大ESG投资。较低的市场化程度和较高的媒体关注程度将会强化网络安全风险对企业ESG投资的正向影响。机制检验表明，网络安全风险较高的企业能够通过增大ESG投资，为其潜在的声誉风险进行“保险”。在面临网络安全风险时，声誉风险敞口越大的企业越有可能增大ESG投资。异质性检验发现，网络安全风险对企业ESG投资的正向影响在供应链集中度较低、管理层短视倾向较低和信息技术背景高管较多的样本中更显著。研究结论有助于理解企业通过ESG投资进行网络安全风险管理的内在逻辑，为鼓励和引导企业坚持“科技向善”的发展战略提供了经验证据。

关键词: 网络安全风险；ESG投资；声誉保险机制；市场化程度；媒体关注
中图分类号: F270 **文献标识码:** A **文章编号:** 1001-4950(2025)04-0003-18

一、引 言

随着数字经济时代的到来，数字技术正在以前所未有的速度与社会各个领域深度融合，与此相伴而生的网络安全问题成为社会和企业必须面对的重大挑战。据IBM Security发布的《数据泄露成本报告》[①]显示，2023年全球数据泄露的平均成本高达445万美元，这一数字不仅刷新了报告发布以来的最高纪录，而且较过去三年增长了15%。在同一时期，因检测安全漏洞及其恶化而产生的成本更是激增了42%。网络安全事件不仅会导致企业运营中断和财务损失，更深远的后果在于对企业声誉的长期侵蚀，削弱利益相关者对企业的信任（Janakiraman等，2018；Kamiya等，2021；Zhu等，2024）。例如，Verizon在谈判收购雅虎时，后者遭遇了大规模的数据泄

收稿日期: 2024-04-17
基金项目: 国家自然科学基金重点项目（71832008）
作者简介: 张才师（1997—），男，上海交通大学安泰经济与管理学院博士研究生；
刘 益（1961—），女，上海交通大学安泰经济与管理学院教授（通信作者，liuyi76@sjtu.edu.cn）。
①https://www.ibm.com/reports/data-breach。

露(30亿条用户信息被盗),导致交易推迟的同时售价下降了9.25亿美元(Zhu等,2024)。蔚来汽车因服务器配置错误导致数百条用户信息泄露,并遭受225万美元等额比特币的勒索,对企业的声誉造成了严重的破坏[①]。美国网络安全公司CrowdStrike的软件漏洞更是导致了全球范围内微软Windows系统的崩溃,全球近3万家企业客户以及政府机构受到影响,媒体将此称为"史上最大规模IT故障",微软公司的安全性再次被推上风口浪尖[②]。因此,探索如何减轻网络安全事件对企业声誉的负面影响,已成为市场和学术界共同关注的紧迫议题。

ESG作为一种可持续和负责任的发展观,强调企业将环境、社会和治理方面的考虑纳入日常的管理和财务决策中。近年来,ESG理念正引导企业重新塑造经营理念,ESG投资越来越被企业和资本市场参与者视为企业重要的战略组成要件(张泽南等,2024)。特别是,ESG投资潜在的风险管理功能正逐渐成为企业应对不确定风险的重要途径(Eisenkopf等,2023;李国栋,2024)。利益相关者理论认为,企业良好的ESG投资表现可以通过获得利益相关者的支持与信任来积累声誉资本,从而有效对冲负面事件发生时企业所可能的声誉损失,形成声誉保险的功能(傅超和吉利,2017;Zhu等,2024)。那么,企业在面临网络安全风险时,是否会通过增加ESG投资来预防网络安全事件发生后所产生的声誉损失?并且,基于美国上市公司数据的研究表明,企业在社会责任方面的卓越表现确实能够在诸如数据泄露等网络安全事件爆发后,显著减轻这些事件所引发的负面影响(Zhu等,2024)。因此,网络安全风险可能是促使企业重视ESG投资的一项重要动因。

基于上述分析,本文旨在深入探讨网络安全风险对企业ESG投资决策的具体影响机制,同时在制度理论的框架内,探究市场化程度和媒体关注程度的调节作用。为了识别网络安全风险对企业ESG投资的影响,本文在Lattanzio和Ma(2023)以及耿勇等(2024)研究的基础上利用Python通过文本分析的方式构建企业的网络安全风险敞口指标。研究发现,网络安全风险越高的企业,越有可能增大ESG投资。较低的市场化程度和较高的媒体关注程度将会强化网络安全风险对企业ESG投资的正向影响。机制检验表明,网络安全风险较高的企业能够通过增大ESG投资,为其潜在的声誉风险进行"保险"。在面临网络安全风险时,声誉风险敞口越大的企业越有可能增大ESG投资。异质性检验显示,网络安全风险对企业ESG投资的正向影响在供应链集中度较低、管理层短视倾向较低和信息技术背景高管较多的样本中更显著。

和以往研究相比,本文主要的理论贡献体现在以下几个方面。(1)相较于国外在网络安全风险领域研究的快速进展,国内由于数据获取的限制,相关领域的实证研究显得相对不足。本文在Lattanzio和Ma(2023)以及耿勇等(2024)研究的基础上,创新性地从文本角度对中国企业网络安全风险指标的构建进行了有益的探索,为国内网络安全风险的相关研究提供了实证借鉴。根据《数字中国发展报告(2023年)》,2023年中国的数字经济规模已超过55万亿元,是世界第二大数字经济体。作为数字经济发展的重要载体,在中国背景下研究网络安全风险的应对战略,无论是对中国数字经济的健康发展,还是对新兴国家发展数字经济都具有重要的启示意义。(2)尽管现有部分文献已经探讨了企业在网络安全风险管理上的多样化策略,包括对信息技术的投资(Angst等,2017)、策略性网络安全保险的采购(Bodin等,2018),以及CEO在企业网络安全事件发生时的应对性道歉(Demek和Kaplan,2023),但ESG投资在网络安全风险管理中的关键作用尚未得到充分探讨。本研究着眼于ESG投资的声誉保险功能,将其视为企业网络安全风险管理的关键组成部分,为网络安全风险管理领域的研究提供了新的理论视角。(3)既有研究主要探讨了ESG投资的直接经济后果,强调其在价值创造上的贡献(宋科等,2022;Chen和

①https://baijiahao.baidu.com/s?id=1752783432959898099&wfr=spider&for=pc。
②https://baijiahao.baidu.com/s?id=1805002956034093375&wfr=spider&for=pc。

Xie，2022；张泽南等，2024）。相较之下，本研究从ESG投资的声誉保险功能这一独特视角出发，发现了其在维护而非仅仅创造企业价值方面的独特作用，为ESG投资潜在经济价值的研究领域增添了新的维度。（4）本文为企业如何在不断变化的市场和制度环境中应对网络安全风险，提出了一个更为全面的分析框架。通过将企业的网络安全风险管理策略选择与其所处的制度背景相结合，本文揭示了企业在不同市场化程度和媒体环境下如何策略性调整其ESG投资，以有效应对网络安全风险。

二、理论分析与假设发展

（一）企业网络安全风险的相关研究

网络安全风险是指外部攻击导致信息技术系统故障，进而引发公司财务损失、业务中断或声誉受损的风险（Florackis等，2023）。网络安全风险的例子包括丢失敏感数据的风险，公司网络、系统和服务的中断，以及物理电子器件的损坏。企业要实现网络安全需要确保的数据信息不被窃取和篡改、软硬件处于安全和可使用状态、数字系统整体安全稳定运行（王秉等，2024）。在当今数字化迅猛发展的时代，随着企业对数字技术的依赖日益加深，网络安全风险正迅速上升为企业面临的主要风险之一。国际学术界主要从两个维度对这一问题进行了深入探讨：一是网络安全风险的经济后果，二是企业的网络安全风险管理战略。一方面，研究发现网络安全风险将会给企业带来广泛而深远的负面影响。网络安全风险不仅侵蚀企业的劳动生产率（Tetteh和Otioma，2024）和研发回报率（Lattanzio和Ma，2023），还会进一步恶化企业在资本市场的表现（Amir等，2018；Florackis等，2023），给企业带来巨大的声誉成本（Kamiya等，2021）。另一方面，学术界和业界正在积极探求应对网络安全风险的有效战略。例如，Bodin等（2018）认为组织无法消除所有网络安全风险以实现百分之百的安全性，组织需要投资网络安全保险，以转移与未来潜在漏洞相关的网络安全风险。Demek和Kaplan（2023）研究发现网络安全风险管理是企业的一项战略举措，并且在应对网络安全漏洞时，CEO的公开道歉会对投资者的投资印象产生积极影响。Angst等（2017）研究发现扩大信息技术投资并不能直接降低数据安全漏洞的发生率。此外，少量的国内研究对中国企业的网络安全风险问题进了有益的探索。耿勇等（2024）通过对中国上市企业网络安全风险的年报披露信息分析表明，企业网络安全风险的增加将会消减供应链伙伴之间信任关系。

本研究聚焦于探讨网络安全风险与企业ESG投资之间的相互关系。现有文献已对此议题进行了初步探索，并揭示了ESG投资在缓解网络安全风险方面的潜在战略价值。Zhu等（2024）根据美国上市公司的数据泄露事件研究发现，企业的内部社会责任无论对预防数据泄露还是减轻数据泄露事件后果都具有重要作用。他们提出企业社会责任可以产生积极的光环效应提升企业声誉，而针对这些公司的网络攻击可能会被视为违反社会规范。D'Arcy等（2020）根据利益相关者理论，将员工和外部黑客定位为公司在网络安全方面的关键利益相关者，并发现试图掩盖不良社会绩效的"漂绿"行为（如慈善捐赠）会使得公司成为安全漏洞的有吸引力的目标。这些发现为我们研究企业网络安全风险与ESG投资之间的关系提供了理论和文献基础。

（二）ESG的相关研究

ESG理念旨在同时考虑各利益相关者的利益，表明组织没有以牺牲对员工、客户、环境和整个社会的责任为代价，将其商业模式推向追求纯粹利润的方向（张泽南等，2024）。将ESG考虑纳入商业决策，实现将商业部门的价值创造活动与可持续发展目标保持一致已经成为社会经济发展的共识。迄今为止，大量实证文献研究了ESG投资与企业绩效之间的关系。然而，在这些文献中却盛行着两种不同的观点。一方面，竞争优势理论和利益相关者理论认为，ESG投资

可以通过帮助企业创造差异化的竞争优势来弥补额外的投入成本。宋科等(2022)的研究发现,ESG投资产生的声誉溢出效应能够提升银行的流动性水平。Chen和Xie(2022)的研究以2000年至2020年中国上市公司为样本,发现在消除内生性问题后ESG披露对公司财务业绩存在显著正向影响。另一方面,基于代理理论和权衡理论的观点认为,ESG活动带来代理问题和资源配置效率低下带来的额外成本,将会使公司在市场竞争中处于不利地位。Nollet等(2016)的研究以2007年至2011年标普500公司为样本,发现了企业社会责任表现和财务业绩存在负相关的证据。Garcia和Orsato(2020)的研究在区分不同国家制度背景的基础上发现,在新兴市场国家,企业的ESG表现与财务业绩之间存在负相关关系。

针对上述矛盾的观点,有部分文献指出,当ESG投资不能给企业产生直接的经济效益时,也可以在未来起到声誉保险作用(傅超和吉利,2017;Shiu和Yang,2017;Zhu等,2024)。ESG在文献中被定义为旨在改善社会条件的公司自愿行为,这些行为试图促进社会公益,并超越公司单一的经济利益(黄珺等,2023)。ESG的自愿性质意味着它能够向利益相关者发出利他主义的信号,表明公司并非完全自私,其管理层将在决策中考虑对他人或社会利益的影响。而当外部利益相关者接收到此类信号时,公司就会累积道德资本(Simon,1995)。当负面事件发生时,基于ESG投资的道德资本能够促使利益相关者将负面事件归因于运气不好而非恶意,并相应地缓和他们的负面反应,从而为企业提供"保险般"的保护(Godfrey等,2009)。从这一观点来看,当企业面临较高的网络安全风险时,企业有动机增大ESG投资来实现风险对冲。

(三)研究假设

当企业遭遇网络安全事件时,除了会产生运营中断以及财务成本等显性成本,更重要的是会对声誉造成极大的伤害(Kamiya等,2021)。首先,网络安全事件将会向利益相关者传递企业缺乏责任的信号。发生网络安全事件在很大程度上意味着企业在网络安全方面的审计标准、员工培训、基础设施以及内部规范存在严重缺陷,企业缺乏足够的努力致力于透明和负责任的运营(Zhu等,2024)。其次,网络安全事件将会向利益相关者传递企业缺乏能力的信号。在网络安全的背景下,现有研究提出了各种威慑机制,例如强大的数字监控和检测技术,能够向内部员工和外部黑客发出信号,表明一个组织的信息和数字资产受到良好保护(Angst等,2017)。相反,如果企业发生了网络安全事件,利益相关者更有可能认为企业缺乏足够的数字技术能力来维护数字信息和数字资产的安全。因此,随着网络安全风险的日益增长,企业面临的声誉风险亦随之上升。这一趋势可能促使企业采取更为前瞻性的策略,通过建立声誉蓄水池来预防不可预见的网络安全事件。

ESG投资的声誉保险理论认为,企业良好的ESG投资表现可以通过获得利益相关者的支持与信任来积累声誉资本,从而能够为企业将来发生负面事件时提供"保险般"的保护(傅超和吉利,2017;Zhu等,2024)。ESG投资向利益相关者发出了一个企业非完全自利的信号,利益相关者会赋予企业道德价值。这些道德价值就构成了企业的声誉资本,进而有利于企业在利益相关者心中形成良好公民的形象。因此,对于那些在ESG方面表现优异的企业,当遭遇网络安全事件时,其已建立的良好公民形象和声誉资本能够有效缓解利益相关者对事件的负面看法,并形成积极归因来保护基于关系的资产免受损失,从而为企业声誉提供"保险般"的保护(Shiu和Yang,2017)。卓越的ESG表现意味着企业杰出的商誉、员工敬业度、产品技术能力以及财务实力,这可能会让消费者相信公司不应为网络安全事件负责,并让投资者相信公司在危机中具有韧性(Eisenkopf等,2023)。此外,相较于其他经营风险,网络安全风险的特殊性也促使企业更加迫切地需要通过增加ESG投资构建声誉蓄水池。首先,企业网络安全风险的波及面广。网络安全事件不仅会对公司本身造成恶劣影响,还有可能进一步传播到其客户和供应商组织(耿勇

等，2024）。这种广泛的波及面要求企业必须向所有利益相关者展示其网络安全防护能力，而ESG投资涉及员工、客户以及政府等广泛利益群体，能够增强所有利益相关者对企业的信任。其次，企业网络安全风险管理的复杂性较高。网络安全风险管理需要综合考虑技术、人员、流程和政策等多个方面，利益相关者通常难以直接观察企业在维护网络安全方面的努力程度（Angst等，2017），并且缺乏评估企业的网络安全风险水平的知识和能力。而ESG投资作为展示企业负责任形象的关键途径，能够更为直接和透明地向外界传达企业在网络安全方面的承诺和专业能力。

基于上述分析，我们认为，为了应对网络安全事件的声誉风险，企业将会通过增大ESG投资来获取声誉资本，从而起到类似保险的作用。更重要的是，ESG投资能提升企业价值的程度，这取决于公司是否需要利用其保险效应。Godfrey（2009）表明保险作为一种风险管理形式，财务困境的成本越高，其价值就越高。这也就意味着，企业的网络安全风险越高，ESG投资所累积的声誉资本的保险价值也就越高。而当企业面临的网络安全风险较低时，企业缺乏足够的动机进行额外的ESG投资构建声誉蓄水池。即面临网络安全风险敞口越大的企业，越有可能增大ESG投资。据此，本文提出假设1。

假设1：企业所面临的网络安全风险对企业的ESG投资具有正向影响。

制度理论认为，企业所处的制度环境在一定程度上影响了企业的战略决策（Young等，2014）。制度背景提供了文化规则和资源，而企业的决策选择是建立在这些规则和资源的基础上（徐细雄等，2020）。因此，在探讨企业网络安全风险与ESG投资之间的关系时，需要进一步考虑企业所处的制度背景。以往的研究表明，市场化程度和媒体关注是解释我国制度背景的重要方面（Wang等，2015；吴先聪和郑国洪，2021；Yang和Jiang，2023）。一方面，相较于西方成熟市场，我国制度环境建设还不够完善，各地区的市场化程度差距较大，对企业的经营决策产生了深刻影响（Wang等，2015）。另一方面，在正式制度缺失的情况下，媒体治理作为我国市场发展中的重要补充在规范和引导企业治理方面发挥着重要的作用（Jeong和Kim，2019）。因此，本文进一步探讨了市场化程度和媒体关注对网络安全风险与企业ESG投资之间关系的调节效应。

尽管我国的市场化转型已经取得了巨大的成就，但是由于经济文化和地理位置等因素，各地区的市场化程度差异较大。总体而言，东部沿海地区市场化程度较高；在中西部地区，非市场因素在资源配置过程中仍然发挥着重要作用（Wang等，2015）。在一个不完美的市场中，ESG作为一种非正式的制度安排可以在一定程度上弥补市场的缺陷（Zhu等，2024），并且ESG投资的收益将随着这些制度的改善而减少。因此，本文认为，在市场化程度较高的地区，ESG投资在管理网络安全风险方面的效用可能会有所降低。一方面，在市场化程度较高的地区，较为完善的法治和市场环境，能够通过强力的监管和严厉的处罚有效威慑内外部网络入侵者，减小企业发生网络安全事件的可能。另一方面，在市场化程度较高的地区，法律作为一种社会强制性规范成为约束市场参与者行为的主要秩序。当网络安全事件发生时，利益相关者更加依赖于通过法律途径解决争议。客观公正的法律制度能够通过明确的责任界定，维护企业在网络安全事件中的合法权益，减少网络安全事件对企业声誉的负面溢出效应。因此，在市场化程度较高的地区，企业可以依靠成熟的外部市场制度来应对网络安全风险；而在市场制度不完善的情况下，企业更依赖于ESG投资来缓解网络安全事件可能带来的声誉损失。据此，本文提出假设2。

假设2：市场化程度减弱了网络安全风险对企业ESG投资的正向影响。

媒体作为社会信息传播的主要媒介，是一种重要的外部市场治理机制。其中，声誉治理机制是媒体发挥外部治理功能的重要的途径（吴先聪和郑国洪，2021），媒体报道通过扩大社会关注影响企业形象，从而改善企业行为。具体而言，媒体关注可能通过两种方式影响网络安全风

险与企业ESG投资之间的关系。一方面，根据风险的社会放大框架，在现实社会中，风险的感知和评估往往受到多种因素的影响，包括个人的心理状态、社会文化背景、媒体传播等，这些因素共同作用可能导致某些风险被过度放大或忽视（Kasperson等，2022）。例如，傅祥斐等（2024）的研究发现，当并购活动受到的社交媒体讨论越负面，公司越有可能终止并购交易。因此，大量的媒体报道可能会放大利益相关者对企业网络安全事件的风险感知，进而增大企业潜在的声誉风险敞口。另一方面，媒体关注同样也会放大ESG投资的声誉保险效应。由于我国社会的集体主义文化取向，媒体关注在塑造我国企业社会责任活动方面扮演着至关重要的角色（Yang和Jiang，2023）。在这种文化背景下，利益相关者会更加信任那些被媒体称为对社会负责任的企业。媒体对企业ESG实践活动的大量报道，能够更有效地帮助企业在利益相关者认知中建立负责任的企业形象，从而与ESG表现较差的企业形成区分。综上可知，媒体关注不仅会放大企业网络安全事件所产生的声誉风险敞口，同时也会增强ESG投资的声誉保险效应，从两方面同时加强高网络安全风险企业增大ESG投资的动机。据此，本文提出假设3。

假设3：媒体关注强化了网络安全风险对企业ESG投资的正向影响。

三、研究设计

（一）样本选择和数据来源

本文以2010—2022年中国A股上市公司为研究对象。我们从深圳证券交易所、上海证券交易所官方网站获取和整理了上市公司年报，基于Python文本挖掘构建相关语义特征词库，形成企业网络安全风险的相关文本词频测度数据。企业ESG评分数据来自万得数据库（Wind）的华证ESG评级，媒体报道数据来自中国研究数据服务平台（CNRDS），市场化指数来自樊纲等编制的“中国分省份市场化指数”，其他数据来自国泰安数据库（CSMAR）。同时本文对初始样本进行如下步骤处理：（1）剔除ST、*ST、PT类非正常交易上市公司；（2）剔除金融类企业；（3）剔除相关指标缺失的样本；（4）为减少异常值影响，对所有连续变量进行1%和99%的缩尾处理。经数据处理后，总计得到3 715家公司的31 366个年度观测值。

（二）变量说明

1.被解释变量。ESG投资（*ESG*），本文选取上市公司覆盖面较广，同时受到以往ESG研究广泛认可的华证ESG指数作为企业ESG投资表现的评估（宋科等，2022；雷雷等，2023）。从构建方法来看，华证指数从环境、社会和公司治理三个维度共选取了16个二级指标和44个三级指标，对企业的ESG表现进行了全面客观的评价。华证ESG指标体系将企业的ESG评分评价为C至AAA九档等级。为方便实证分析，本文将企业ESG评级根据等级分别赋值为1至9分，并使用当年的季度平均值作为企业ESG表现的衡量。

2.解释变量。企业网络安全风险（*Cybersecurity*），在数字化高速发展的时代，网络安全已成为一个不可忽视的重要议题（Florackis等，2023）。随着网络和信息技术的广泛应用，企业面临网络攻击、数据泄露、隐私保护等挑战。然而，由于缺乏企业层面网络安全事件的相关数据，当前国内网络安全相关的实证研究较少。最近，少部分研究基于机器学习方法，通过对企业披露的年报文本进行文本分析，构建了企业面临的网络安全风险指标（Lattanzio和Ma，2023；耿勇等，2024）。年报中的词汇用法能够折射出企业的战略特征和未来展望（吴非等，2021），网络安全风险作为新时代下企业所面临的重要挑战之一，这类特征信息更容易体现在企业具有总结和指导性质的年报中。此外，中国证券监督管理委员会要求中国上市公司在年报中对企业所面临的各种风险进行说明，因此，对于那些网络安全风险较高的企业，管理层为了降低未来可能面临的监管处罚，有动机在年报中向利益相关者传达他们关于网络安全风险的担忧（Lattanzio

和Ma，2023；Chen等，2023；耿勇等，2024）。这为我们利用公司年报中的网络安全相关的披露信息来构建企业面临的网络安全风险指标提供了依据。在现有文献的基础上，本文邀请两名网络安全领域的专家使用Lattanzio和Ma（2023）以及耿勇等（2024）开发的网络安全风险词典和工信部网络安全管理局的相关政策文件，共同归纳整理出包含网络攻击、数据泄露等73个与网络安全风险相关的词语作为本文的关键词词典[①]。最后，基于Python对上市公司年报中管理层分析与讨论文本进行关键词搜索、匹配和词频计数，计算得到73个与企业网络安全风险相关的词汇在年报中的出现频率，进而使用加总词频的对数作为企业网络安全风险的测量。

3.调节变量。市场化程度（*Market*），樊纲等（2011）构建的中国分省份市场化指数从市场化的5个不同方面，包括政府与市场的关系、非国有经济的发展、产品市场的发育程度、要素市场的发育程度以及市场中介组织的发育和法律制度环境，对全国各省级行政区的市场化程度进行了评估。本文选取企业总部所在省份的市场化指数作为市场化程度的测量。媒体关注（*Media*），参考郭檬楠等（2023），本研究以全年网络新闻内容中出现该企业的新闻总数来度量企业的媒体关注程度。此外，为了使媒体关注程度更符合正态分布，还进行了加1后取自然对数处理。新闻数据来源于CNRDS，该数据平台中的网络新闻包括了来自400多家重要网络媒体的新闻报道数据，包括新浪财经、东方财富网、腾讯财经、网易财经等主流网络财经媒体的新闻报道。

参考以往对企业ESG投资影响因素的研究（雷雷等，2023；Feng和Yuan，2024），本文还控制了盈利能力（*Roa*）、企业规模（*Size*）、财务杠杆（*Lev*）、企业性质（*SOE*）、企业年龄（*Age*）、股权集中度（*Top1*）、董事会规模（*Board*）、管理所有权（*Mholdings*）、现金持有（*Cash*）、资本支出（*Capex*）和产品市场竞争（*HHI*）等控制变量。此外，本文还控制了行业固定效应（Ind）和年份固定效应（Year），以消除不同年份和行业之间的差异。变量具体定义如表1所示。

表 1　变量定义

变量类型	变量名称	变量符号	变量定义
被解释变量	ESG投资	*ESG*	华证ESG评分年均值
解释变量	网络安全风险	*Cybersecurity*	年报网络安全风险相关的词频数，加1取对数
调节变量	市场化程度	*Market*	樊纲等编制的“中国市场化指数”
	媒体关注	*Media*	当年新闻内容中出现该企业的总数，加1取对数
控制变量	盈利能力	*ROA*	净利润/总资产
	企业规模	*Size*	总资产，取对数
	财务杠杆	*Lev*	总负债/总资产
	企业性质	*SOE*	国有企业取1，否则取0
	企业年龄	*Age*	成立年限，取对数
	股权集中度	*Top1*	第一大股东持股比例
	董事会规模	*Board*	董事会人数，取对数
	管理所有权	*Mholdings*	管理层持股比例
	现金持有	*Cash*	现金及现金等价物余额/总资产
	资本支出	*Capex*	购建固定资产、无形资产和其他长期资产支付的现金/总资产
	产品市场竞争	*HHI*	行业赫芬达尔指数

①企业网络安全风险的关键词包括：网络安全、网络攻击、网络威胁、网络钓鱼、网络弹性、网络韧性、网络事件、网络事故、网络窃听、网络欺诈、安全事件、入侵、加密、黑客、防火墙、安全漏洞、内部威胁、云安全、信息风险、信息安全、信息泄露、信息系统、数据安全、数据完整、数据备份、数据加密、数据滥用、数据篡改、数据共享风险、数据隐私、数据泄露、数据资产、IT资产、数据盗窃、数据窃取、数据丢失、计算机安全、计算机病毒、计算机漏洞、电脑漏洞、病毒软件、木马病毒、恶意软件、恶意程序、勒索软件、间谍软件、赛博攻击、脚本攻击、计算机攻击、系统安全、系统完整、安全监控、安全审计、安防监控、安全支出、安全措施、安全策略、安全协议、安全认证、安全架构、安全法规、安全培训、加密技术、弱密码、未经授权、访问控制、漏洞扫描、身份验证、非授权访问、越权访问、非法访问、访问权限、越权存取。

（三）模型设定

为检验假设1，参考雷雷等（2023）以及Feng和Yuan（2024）的研究，本文设定了如下模型来检验网络安全风险与企业ESG投资的关系。

$$ESG_{i,t}=\beta_0+\beta_1 Cybersecurity_{i,t}+Control_{i,t}+Ind+Year+\varepsilon_{i,t} \quad (1)$$

其中，$ESG_{i,t}$为i企业在t期的ESG投资表现；$Cybersecurity_{i,t}$为i企业在t期所面临的网络安全风险水平；$Control_{i,t}$为控制变量；Ind和$Year$分别为行业虚拟变量和年份虚拟变量；$\varepsilon_{i,t}$为随机扰动项。本文重点关注回归系数β_1，若假设1成立，则β_1，显著大于0。

为检验假设2和假设3，在模型（1）的基础上，分别加入了市场化程度（$Market$）以及其与网络安全风险水平的交互项（$Cybersecurity\times Market$）、媒体关注（$Media$）以及其与网络安全风险水平的交互项（$Cybersecurity\times Media$），构建模型（2）和模型（3），如下所示。

$$ESG_{i,t}=\alpha_0+\alpha_1 Cybersecurity_{i,t}+\alpha_2 Market_{i,t}+\alpha_3 Cybersecurity_{i,t}\times Market_{i,t}+Control_{i,t}+Ind+Year+\varepsilon_{i,t} \quad (2)$$

$$ESG_{i,t}=\gamma_0+\gamma_1 Cybersecurity_{i,t}+\gamma_2 Media_{i,t}+\gamma_3 Cybersecurity_{i,t}\times Media_{i,t}+Control_{i,t}+Ind+Year+\varepsilon_{i,t} \quad (3)$$

本文重点关注模型（2）中的交互系数α_3和模型（3）中的交互系数γ_3，若假设2和假设3成立，则α_3显著小于0，γ_3显著大于0。

四、实证分析

（一）企业网络安全风险指标有效性检验

为验证本文所开发的网络安全风险指标能够准确映射企业实际所面临的网络安全风险，参考耿勇等（2024），本研究从测量指标的行业分布特征、时间变化趋势以及经济合理性三个方面进行了深入的检验分析。

首先，本文考察了企业网络安全风险识别指标在不同行业中的分布特征。为确保分析的代表性，本文排除了样本数量不足100个的行业。分析结果显示（相关图表限于篇幅未列示，备索），网络安全风险在各个行业间表现出明显差异。在软件和信息技术服务业，航空运输业，互联网和相关服务业，计算机、通信和其他电子设备制造业，以及电信、广播电视和卫星传输服务业等更依赖于网络信息技术的行业，网络安全风险的问题尤为突出。相比之下，纺织业、农业以及生态和环境治理行业等信息化水平较低的行业，面临的网络安全风险则相对较小。因此，该结果进一步证实了本文所采用的测量指标与网络安全风险在各行业中的分布特征相吻合。

其次，本文考察了企业网络安全风险识别指标的时间变化趋势，并将其与企业数字化转型[①]的进程进行了同期对比，相关结果展示在图1中。从数字化发展趋势来看，企业的网络安全风险与数字化转型的步伐呈现出基本一致的演变趋势。从网络安全治理的角度观察，我们注意到，在若干关键网络安全法律法规实施的时间节点，企业遭遇的网络安全风险普遍得到了缓解。例如，2015年我国首部全面规范网络空间安全管理方面问题的基础性法律——《中华人民共和国网络安全法》（草案）在中国人大网上全文公布，有效遏制了网络安全问题的扩散。因此，图1的结果证实了本文提出的测量指标与网络安全风险的时间变化趋势存在显著的一致性。

最后，本文深入分析了企业网络安全风险识别指标的经济合理性。网络安全风险为企业的生产和运营带来了额外的不确定性，这将会增加企业的风险承担水平和经营风险。因此，一个有效的网络安全风险指标对于识别和预测企业所面临的风险至关重要。为了验证该指标的有

①本文通过参考吴非等（2021）的做法，通过对企业年报中数字化相关的关键词进行搜索、匹配和统计得到企业数字化转型的指标。

效性，本文进一步评估了网络安全风险对企业风险承担水平和经营风险的影响。为了量化这一影响，本文使用企业经行业调整的ROA三年滚动标准差（Cao等，2023）以及Z指数（司登奎等，2023）分别反映企业的风险承担水平和经营风险。根据表2可知，网络安全风险增大了企业当前和未来一期的盈利波动性（*Risk*），同时减小了企业当前和未来一期的Z指数（*Z-Socre*）。表2的结果表明，网络安全风险显著增大了企业的风险承担水平和经营风险，从而证明了本文所构建的网络安全风险指标在经济上的合理性和实际应用价值。

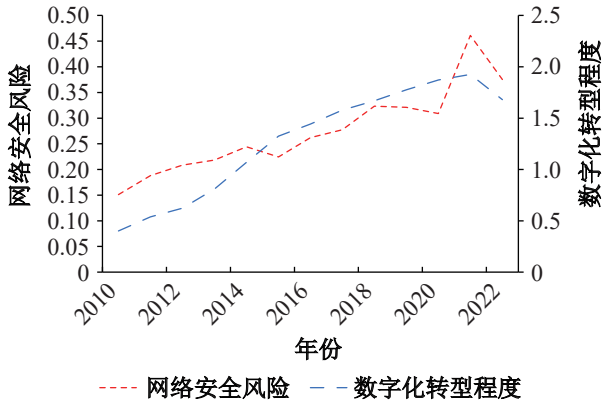

图 1　网络安全风险时间趋势

表 2　网络安全风险与企业经营风险

	（1）	（2）	（3）	（4）
	$Risk_t$	$Risk_{t+1}$	$Z\text{-}Socre_t$	$Z\text{-}Socre_{t+1}$
Cybersecurity	0.001**	0.001**	−0.451***	−0.533***
	（2.28）	（2.13）	（−2.80）	（−2.81）
常数项	0.395***	0.267***	31.662***	34.023***
	（24.55）	（14.89）	（14.72）	（13.93）
控制变量	控制	控制	控制	控制
年份效应	控制	控制	控制	控制
行业效应	控制	控制	控制	控制
观测值	29 552	25 307	28 827	25 017
$Adj.R^2$	0.37	0.37	0.11	0.10

注：括号内为*t*值；***、**和*分别表示在1%、5%和10%的水平上显著。下同。

（二）主要变量描述性统计

表3是主要变量的描述性统计。结果显示，企业ESG投资表现（*ESG*）的均值为4.098，标准差为1.021，表明我国上市企业的投资表现总体水平较低，不同企业之间ESG投资表现的差异较大。企业网络安全风险水平（*Cybersecurity*）的均值为0.286，标准差为0.574，呈现出标准差大于均值的特点，表明不同企业间的网络安全风险水平差异较大。因此，研究网络安全风险对企业ESG投资的影响存在重要意义，其他变量的量纲与现有文献保持一致。

（三）多元回归结果分析

表4为多元回归模型的结果，包含主效应模型和交互效应模型分析。表4列（1）报告了仅包含解释变量和控制变量的结果，结果显示网络安全风险与企业ESG投资的估计系数为0.063，且在1%的水平上显著。即当企业所面临的网络安全风险越高，在一定程度上决定了其面临的声誉风险敞口越大，ESG投资所起到的声誉保险作用也就越大，进而促使企业增大ESG投资。

由此可知，企业网络安全风险对企业ESG投资存在显著的正向影响，验证了本文的假设1。

表 3　描述性统计结果

变量	观测值	均值	标准差	最小值	中值	最大值
ESG	31 366	4.098	1.021	1.250	4.000	6.000
Cybersecurity	31 366	0.286	0.574	0.000	0.000	2.773
Market	31 366	9.580	1.703	4.076	9.835	12.390
Media	31 366	4.930	1.134	0.000	4.920	7.842
ROA	31 366	0.039	0.063	−0.261	0.039	0.205
Size	31 366	22.154	1.304	19.803	21.959	26.190
Lev	31 366	0.416	0.208	0.050	0.406	0.922
SOE	31 366	2.876	0.341	1.792	2.944	3.497
Age	31 366	0.359	0.480	0.000	0.000	1.000
Top1	31 366	0.342	0.148	0.088	0.320	0.738
Board	31 366	2.129	0.198	1.609	2.197	2.708
Mholdings	31 366	0.104	0.173	0.000	0.000	0.665
Cash	31 366	0.170	0.134	0.011	0.131	0.661
Capex	31 366	0.051	0.047	0.001	0.037	0.228
HHI	31 366	0.104	0.110	0.017	0.072	0.731

表 4　网络安全风险、外部治理环境与ESG投资

	（1）	（2）	（3）	（4）
	ESG	*ESG*	*ESG*	*ESG*
Cybersecurity	0.063***	0.071***	0.063***	0.070***
	（6.08）	（6.78）	（6.09）	（6.73）
Market		0.065***		0.064***
		（9.78）		（9.70）
Cybersecurity×Market		−0.036***		−0.035***
		（−3.53）		（−3.41）
Media			−0.011	−0.008
			（−1.44）	（−1.04）
Cybersecurity×Media			0.021**	0.019**
			（2.57）	（2.31）
常数项	−1.569***	−1.539***	−1.611***	−1.563***
	（−11.43）	（−11.38）	（−11.16）	（−10.84）
控制变量	控制	控制	控制	控制
年份/行业效应	控制	控制	控制	控制
观测值	31 366	31 366	31 366	31 366
Adj.R^2	0.22	0.22	0.22	0.22

表4列（2）给出了市场化程度对网络安全风险和企业ESG投资关系的调节作用结果。由列（2）可以发现，交互项回归系数为−0.036，且在1%的水平上显著，说明地区的市场化程度显著减弱了网络安全风险对企业ESG投资的正向影响，假设2得到验证。这表明在市场化程度越高的地区，随着法律和行业规范的不断完善，网络安全事件对企业声誉的负面溢出效应越小，增加ESG投资为企业声誉“保险”的价值减弱。

表4列（3）给出了媒体关注对网络安全风险和企业ESG投资关系的调节作用结果。由列（3）可以发现，交互项回归系数为0.021，且在5%的水平上显著，说明媒体对企业关注程度显著增强了网络安全风险对企业ESG投资的正向影响，假设3得到验证。这表明媒体较高的关注度，不仅能够放大企业网络安全风险的负面后果，形成更大的声誉风险敞口，也能够对企业ESG投资进行解读和散播，放大企业ESG投资的声誉保险价值。

表4列(4)同时加入了市场化程度和媒体关注的交互效应。由列(4)可以发现,网络安全风险与企业ESG投资的估计系数,以及市场化程度和媒体关注的交互项回归系数,均至少在5%的水平上显著,再次验证了本文的假设。

(四)稳健性检验

为了确保研究结论的可靠性,本文进一步采用工具变量法、Heckman两阶段回归、倾向匹配得分法(PSM)、估计方法更换、增加控制变量、关键变量替换等方法进行了稳健性检验。

1.工具变量法。若存在未观测到的因素能够同时影响企业的网络安全风险和ESG投资,那么本文基准回归结果将存在遗漏变量导致的潜在内生性问题。本文选取同年度同地区企业网络安全风险的均值(*IV*)作为工具变量。同地区企业所面临的数字环境与经营环境相一致,因此同地区其他企业网络安全风险的平均水平与该企业的网络安全风险强关联,但并不直接影响该企业的ESG投资,满足工具变量的相关性和外生性要求。表5列(1)给出了工具变量的第一阶段回归结果,显示工具变量与企业网络安全风险在1%的水平下显著正相关,满足相关性要求。列(2)给出了第二阶段的回归结果,与前文的回归结果一致,故前文研究结论具有稳健性。

表 5　稳健性检验结果

	工具变量法		Heckman两阶段		PSM	固定效应模型	控制风险变量
	(1)	(2)	(3)	(4)	(5)	(6)	(7)
	Cybersecurity	*ESG*	*dum_CS*	*ESG*	*ESG*	*ESG*	*ESG*
Cybersecurity		0.348***		0.061***	0.065***	0.038***	0.061***
		(3.25)		(5.92)	(5.13)	(3.59)	(5.80)
IV	0.466***		0.938***				
	(17.22)		(12.26)				
IMR				−0.216**			
				(−3.05)			
Risk							−3.073***
							(−17.44)
Z−Socre							−0.001
							(−1.14)
Litigation							−0.091***
							(−6.83)
常数项	−0.488***	−1.940***	−3.361***	−1.010***	−1.691***	−0.822***	−0.613***
	(−6.57)	(−11.39)	(−13.10)	(−4.49)	(−8.28)	(−2.67)	(−4.29)
控制变量	控制	控制	控制	控制	控制	控制	控制
年份/行业效应	控制	控制	控制	控制	控制	控制	控制
企业效应	不控制	不控制	不控制	不控制	不控制	控制	不控制
观测值	31366	31366	31311	31311	14109	31366	28786
$Adj.R^2/PseudoR^2$	0.25	0.15	0.14	0.22	0.21	0.58	0.21

2.Heckman两阶段回归。样本企业是否存在网络安全风险会受到企业的多种内外部因素影响,由此筛选的样本可能会产生估计偏误。因此,本文使用Heckman两阶段法来检验可能存在的样本自选择问题。在Heckman第一阶段的Probit回归模型中,按照样本企业是否存在网络安全风险生成虚拟变量*dum_CS*,若存在网络安全风险则编码为1,否则取0。在保持原有模型全部控制变量的基础上,我们加入工具变量(*IV*)进行回归得到逆米尔斯比率(*IMR*)。在第二阶段中,将逆米尔斯比率(*IMR*)作为控制变量加入原有模型中进行回归分析。从表5列(3)和列(4)可知,第一阶段中同地区企业网络安全风险的均值(*IV*)与虚拟变量(*dumDSR*)在1%的显著性水平下正相关,表明工具变量对虚拟变量的解释力度较大。第二阶段中,在控制逆米尔斯比率

后，相关回归结果与前文结果一致，说明本文主要结论依旧稳健。

3.倾向匹配得分法（PSM）。由于企业所面临的网络安全风险不是随机的，网络安全风险较高和较低的企业之间可能存在系统性差异。为了消除这些潜在差异所产生的内生性问题，我们进一步采用倾向得分匹配法（PSM）来重新检验网络安全风险与企业ESG投资之间的关系。我们将存在网络安全风险的样本划分为高网络安全风险组，而将不存在网络安全风险的样本划分为低网络安全风险组，采用Logit回归计算倾向得分。在匹配模型中我们加入了模型（1）的控制变量，并采用1∶1最近邻匹配法。PSM匹配后高网络安全风险组和低网络安全风险组的控制变量平均偏差仅为1.5%，且倾向得分共同取值范围较大，匹配样本具备代表性。PSM匹配后的回归结果如表5列（5）所示，与前文回归结果一致。

4.更换估计方法。为了减轻企业不随时间变化的特征对本文回归估计的影响，在上文控制行业和年份固定效应的基础上，本文进一步采用固定效应模型控制公司个体效应。检验结果如表5列（6）所示，得出与上文一致的结论，即随着网络安全风险的增加将会显著增大企业的ESG投资。

5.增加控制变量。考虑到当企业面临其他风险时，也可能通过增大ESG投资来维护企业声誉。因此，为减少企业其他风险对本文结果的干预，我们进一步控制了企业的风险承担水平（*Risk*）、运营风险（*Z-Socre*）和诉讼风险[①]（*Litigation*）。检验结果如表5列（7）所示，在控制住企业的其他风险水平后，得出的结论与上文一致。

6.替换关键变量。本文对被解释变量和解释变量进行替换来检验模型的稳健性。首先，参考雷雷等（2023），本文采用CNRDS ESG评级数据（*CNRDS_ESG*）替换本文主回归中使用的被解释变量衡量指标进行了稳健性检验。CNRDS ESG数据库基于ISO26000、GRI Standards、SASB Standards等国际ESG披露标准和国内外知名ESG数据库的设计思路，并结合中国ESG信息披露的相关政策，构建了独特的中国企业的ESG评分体系。回归结果如表6列（1）至（3）所示，网络安全风险对企业ESG投资的回归系数显著为正，市场化程度与网络安全风险的交互项系数显著为负，媒体关注与网络安全风险的交互项系数显著为正，再次验证了本文的主要结论。其次，考虑到不同公司年报MD&A部分文本长度存在差异，使用总词频可能导致不同公司之间的网络安全风险缺乏可比性，本文使用经年报MD&A 语段长度标准化调整后的词频占比作为网络安全风险（*RCybersecurity*）的替代测量。回归结果如表6列（4）至（6）所示，与上文回归结果一致。

（五）ESG投资的声誉保险机制检验

本部分我们进一步检验了ESG投资对企业网络安全风险的声誉保险机制。上文的假设部分论证了当企业面临较高网络安全风险时，能够通过增大ESG投资来获取声誉资本，从而减小将来网络安全事件发生时所引起的声誉损失，对企业的声誉形成“保险”。这意味着，声誉越高的企业面临网络安全风险时，声誉损失的敞口也就越大，从而也就有着更强动机增大ESG投资来维护企业声誉。参考管考磊和张蕊（2019）对企业声誉的测量，本文从消费者角度、债权人角度、股东角度以及企业角度选择了12个企业声誉评价指标[②]，采用因子分析方法计算出企业声誉得分（*REP_score*），并根据声誉得分的高低将样本划分为十组依次赋值*REP_rank*为1至10。从表7列（1）和列（2）可知，ESG投资有助于企业提升企业声誉。根据表7列（3）和列（4）可知，网络安全风险与企业声誉的交互项系数显著为正，表明声誉越高的企业越有可能增大ESG投资。

①本文参考傅超和吉利（2017）使用企业当年所涉及的诉讼次数取对数，作为企业诉讼风险的衡量。

②消费者和社会角度的指标：企业总资产、营业收入、净利润和企业价值在行业内的排名。债权人角度的指标：资产负债率、流动比率、长期负债比。股东角度的指标：每股收益、每股股利、是否为国际四大会计师事务所审计。企业角度的指标：可持续增长率、独立董事比例。

依据表7所呈现的结果，我们可以得出结论：在遭遇网络安全风险的情况下，那些面临较高声誉风险敞口的企业更加倾向于增加ESG投资。这一现象证实了ESG投资作为一种声誉保护机制的有效性，表明企业通过加强ESG实践来为其潜在的网络安全风险提供声誉保险。

表 6　稳健性检验：替换关键变量

	替换被解释变量			替换解释变量		
	（1）	（2）	（3）	（4）	（5）	（6）
	CNRDS_ESG	*CNRDS_ESG*	*CNRDS_ESG*	*ESG*	*ESG*	*ESG*
Cybersecurity	1.019***	1.126***	0.994***			
	（11.64）	（12.05）	（10.83）			
Cybersecurity×Market		−0.554***				
		（−6.10）				
Cybersecurity×Media			0.157**			
			（2.15）			
RCybersecurity				1.080***	1.172***	1.112***
				（4.32）	（4.68）	（4.44）
RCybersecurity×Market					−0.767***	
					（−3.09）	
RCybersecurity×Media						0.489**
						（2.12）
常数项	−4.081***	−4.221***	−0.515	−1.591***	−1.562***	−1.698***
	（−3.28）	（−3.49）	（−0.40）	（−11.76）	（−11.56）	（−11.89）
控制变量	控制	控制	控制	控制	控制	控制
年份/行业效应	控制	控制	控制	控制	控制	控制
观测值	31 366	31 366	31 366	31 366	31 366	31 366
Adj.R^2	0.43	0.43	0.43	0.22	0.22	0.22

表 7　ESG声誉保险机制检验结果

	（1）	（2）	（3）	（4）
	REP_rank	*REP_score*	*ESG*	*ESG*
ESG	0.116***	0.020***		
	（11.13）	（11.03）		
Cybersecurity×REP_rank			0.011*	
			（1.69）	
Cybersecurity×REP_score				0.089**
				（1.98）**
常数项	−32.948***	−7.511***	−0.052	0.521
	（−133.67）	（−177.62）	（−0.27）	（2.35）
控制变量	控制	控制	控制	控制
年份/行业效应	控制	控制	控制	控制
观测值	24 776	24 776	24 776	24 776
Adj.R^2	0.75	0.81	0.21	0.21

（六）异质性分析

1.供应链集中度的异质性分析

现有文献表明较高的供应链集中度，能够促进企业与利益相关者之间的私人信息交换，从而减轻企业与利益相关者之间的信息不对称程度（Crawford等，2020）。因此，对于供应链集中较高的企业，即使面临较高的网络安全风险，也能够通过私人信息传递来缓解供应链伙伴的担忧，从而减小了ESG投资的信号传递作用和声誉保险价值。本文使用企业前5大供应商、客户采

购销售比例之和的均值作为供应链集中度的测量，并按照中值将样本划分为高供应链集中度企业和低供应链集中度企业进行分组回归检验。回归结果如表8中列（1）和列（2）所示，相较于高供应链集中度企业，低供应链集中度企业中网络安全风险对ESG投资的影响系数增大了0.031，且Bootstrap分组回归系数检验在1%的水平上显著。结果表明，紧密的供应链合作伙伴关系，能够有效减轻网络安全风险对企业声誉的损害，减小了企业增大ESG投资的动机。

表 8　异质性分析结果

	高供应链集中度	低供应链集中度	管理层高短视倾向	管理层低短视倾向	信息技术背景高管较多	信息技术背景高管较少
	（1）	（2）	（3）	（4）	（5）	（6）
	ESG	*ESG*	*ESG*	*ESG*	*ESG*	*ESG*
Cybersecurity	0.046***	0.077***	0.042**	0.080***	0.084***	0.015
	（3.24）	（5.25）	（2.56）	（6.08）	（6.89）	（0.78）
常数项	−1.401***	−2.197***	−1.729***	−1.363***	−1.564***	−1.531***
	（−7.24）	（−5.65）	（−9.05）	（−7.07）	（−8.13）	（−7.97）
控制变量	控制	控制	控制	控制	控制	控制
年份/行业效应	控制	控制	控制	控制	控制	控制
观测值	16 600	14 763	15 678	15 684	15 832	15 530
Adj.R^2	0.22	0.21	0.23	0.21	0.22	0.23
组间系数差异检验	P值=[0.00]		P值=[0.00]			

2.管理层短视的异质性分析

尽管企业在网络安全领域面临着显著的风险，但一些短视的管理者可能会采取机会主义的行为。他们可能会错误地认为网络安全事件在短期内不太可能发生，从而缺乏足够的动机去增加ESG投资。参考胡楠等（2021），本文使用年报MD&A中披露的“短期视域”的词频测算管理层的短视主义，并按照中值将样本划分为管理层高短视倾向的企业和管理层低短视倾向的企业进行分组检验，回归结果见表8中列（3）和列（4）。可以发现，相较于管理层短视倾向较高的企业，管理层短视倾向较低的企业中网络安全风险对ESG投资的影响系数增大了0.038，且Bootstrap分组回归系数检验在1%的水平上显著。结果表明，短视的管理层可能忽视网络安全的长期重要性，减弱了其增大ESG投资来应对网络安全风险的动机。

3.高管信息技术背景的异质性分析

现有研究表明，具备信息技术背景的高管更有可能为企业制定长期发展的数字化转型战略（吴育辉等，2022）。因此，相较于缺乏信息技术经验的高管，拥有信息技术背景的高管更有可能意识到企业在数字化转型过程中积极应对网络安全风险的必要性。本文使用上市公司当年具有信息技术背景的高管占高管团队总人数的比例衡量高管的信息技术背景，并按照中值将样本划分为信息技术背景高管较多的企业和信息技术背景高管较少的企业进行分组检验，回归结果见表8中列（5）和列（6）。可以发现，在缺乏信息技术背景高管的企业中，*Cybersecurity*的系数不显著。结果表明，那些拥有信息技术背景的高级管理人员，往往对网络安全事件的潜在破坏性有着更深刻的认识。这种认识促使他们更加积极地推动企业在ESG方面的前瞻性投资，以预防和缓解网络安全风险所造成的声誉损失。

五、结论与建议

本文以2010—2022年中国A股非金融类上市公司为研究样本，实证检验了网络安全风险对企业ESG投资的影响效应和影响机制，并进一步探讨了市场化程度和媒体关注对二者关系

的调节作用。研究结果表明：(1)网络安全风险越高的企业，越有可能增大ESG投资。网络安全风险和企业ESG投资之间的关系，在市场化程度低以及媒体关注高的市场环境下更为显著。(2)机制检验发现，网络安全风险较高的企业通过增大ESG投资，为其潜在的声誉风险进行“保险”。在面临网络安全风险时，声誉风险敞口越大的企业越有可能增大ESG投资。(3)异质性检验还发现，网络安全风险对企业ESG投资的正向影响在供应链集中度较低、管理层短视倾向较低和信息技术背景高管较多的样本中更显著。本文的研究结论表明，ESG投资是企业管理和应对网络安全风险的一项重要战略工具，并且外部制度环境在其中扮演着重要的角色。这一发现对上市公司本身、监管部门以及中国经济的高质量发展都有着重要的启示意义。

对于上市公司而言，在数字时代背景下，网络安全风险已成为企业不容忽视的关键风险源，对企业的日常运营和持续发展构成潜在威胁。尤为重要的是，网络安全事件可能严重损害企业声誉。本研究表明，通过ESG投资所积累的声誉资本，能够为其潜在的声誉风险进行“保险”。本文的研究结论鼓励企业管理者坚持“科技向善”的长远发展战略，在拥抱数字化的同时坚持负责任的经营理念，以应对不断增长的网络安全风险。例如，为了应对日益增长的网络安全风险以及监管压力，TikTok通过设立透明和问责中心，能够让公众以及监管机构更仔细地了解TikTok如何围绕安全性、数据和隐私做出决策的细节[①]。腾讯公司通过推出公益性质的“守护者计划”，携手监管机构、社会公众以及合作企业共建“网络安全共同体”，不仅体现了腾讯的社会责任，也推动了中国网络安全治理[②]。总之，推动ESG发展，确保在科技发展的同时坚守社会责任，有助于企业在复杂多变的网络环境中保持竞争力和可持续性。

对于监管部门而言，首先，在数字化迅速发展的当下，网络安全风险已成为全球性挑战，对社会经济的稳定和可持续发展构成了严峻威胁。企业作为经济活动的主体，其网络安全管理的优劣直接关联到整个社会的网络安全状况。政府应当进一步加强建设市场化程度高、法制健全的数字营商环境，增加对网络攻击以及网络犯罪的惩戒力度，积极出台和完善相关法律，减小企业面临的网络安全风险以及网络安全事件发生后的维权成本和恢复成本。其次，政府及相关监管机构应该加强对新闻媒体的监管，引导媒体树立正确的舆论导向和价值取向，对网络安全事件进行客观公正的报道，在充分发挥外部监督功能的同时减小企业不必要的声誉损失。媒体在报道时应力求平衡，既揭示潜在风险，也认可企业在网络安全风险管理和透明度方面的努力。最后，ESG体系的建设对于企业识别和管理多元化风险至关重要，不仅涵盖网络安全风险，也包括运营风险等其他关键领域。政府应在推动企业ESG建设方面扮演更加关键的角色，不断强化和完善ESG相关的法规、政策和监管机制。

对于中国经济的高质量发展而言，数字经济与可持续发展已经成为新时代中国经济高质量发展两大动力引擎。以往的观点大多强调了数字经济对于企业可持续发展的促进作用(刘方媛和吴云龙，2024)，然而本文的研究结果表明企业在ESG方面的投资同样能够帮助企业抵御网络安全风险。这表明在新的经济发展形势下，数字经济与可持续发展战略是相辅相成的，这二者构成了中国经济高质量发展的重要内涵。这种互补性不仅揭示了两者内在的联系，而且凸显了它们在推动中国经济向更高质量阶段发展中的核心作用。数字经济通过其创新动力和效率优势，为可持续发展注入了新的活力；而可持续发展的理念则为数字经济的长远发展提供了指导原则和价值导向。两者的有机结合，形成了中国经济高质量发展的坚实基础和显著特征。

本研究仍存在局限性，有待未来继续拓展和探索。首先，本文重点研究了企业面临的网络

①http://ie.mofcom.gov.cn/article/jmxw/202105/20210503061651.shtml。

②https://baike.baidu.com/item/守护者计划/19494376?fr=ge_ala。

安全风险如何影响企业的ESG投资表现。然而，由于数据受限，我们未能检验ESG投资如何影响企业实际发生的网络安全事件以及其是否有助于企业在网络安全事件中恢复，这都有待未来的进一步研究。其次，本研究强调了ESG投资的声誉保险作用，涉及企业社会责任的多个方面，未来的研究可以细化到特定的社会责任维度，例如企业的慈善捐赠、环境保护等方面。此外，本文使用年报词频数据衡量企业整体的网络安全风险。然而，根据入侵者的不同网络安全风险可以分为外部组织威胁和内部员工威胁，不同的风险来源将可能影响企业应对策略的选择，未来的研究可进一步细化网络安全风险的来源。最后，鉴于网络安全风险的普遍性和潜在破坏性，单纯依赖ESG投资并不足以全面应对这些挑战。未来的研究应当探索更为全面和系统的方法来增强企业的网络安全防护。例如，采用模糊集定性比较分析（FQCA）等方法，可以深入探究不同情境下应对网络安全风险的有效战略组合，为企业制定更为科学和有效的网络安全风险管理策略提供理论支持和实践指导。

主要参考文献

[1]樊纲, 王小鲁, 马光荣. 中国市场化进程对经济增长的贡献[J]. 经济研究, 2011, 46(9): 4-16.

[2]傅超, 吉利. 诉讼风险与公司慈善捐赠——基于“声誉保险”视角的解释[J]. 南开管理评论, 2017, 20(2): 108-121.

[3]耿勇, 向晓建, 万攀兵. 供应链信任衰退: 网络安全风险与企业贸易信贷[J]. 中国工业经济, 2024, (5): 135-154.

[4]管考磊, 张蕊. 企业声誉与盈余管理: 有效契约观还是寻租观[J]. 会计研究, 2019, (1): 59-64.

[5]郭檬楠, 贺一凡, 牛建业. 内部控制、网络媒体报道与企业ESG表现[J]. 管理学刊, 2023, 36(3): 103-119.

[6]胡楠, 薛付婧, 王昊楠. 管理者短视主义影响企业长期投资吗?——基于文本分析和机器学习[J]. 管理世界, 2021, 37(5): 139-156.

[7]黄珺, 汪玉荷, 韩菲菲, 等. ESG信息披露: 内涵辨析、评价方法与作用机制[J]. 外国经济与管理, 2023, 45(6): 3-18.

[8]雷雷, 张大永, 姬强. 共同机构持股与企业ESG表现[J]. 经济研究, 2023, 58(4): 133-151.

[9]潘蓉蓉, 罗建强, 杨子超. 制造企业服务化、前后台数字化与企业绩效[J]. 系统管理学报, 2022, 31(5): 988-999.

[10]司登奎, 李小林, 孔东民, 等. 利率市场化能降低企业营运风险吗?——基于融资约束和企业金融化的双重视角[J]. 金融研究, 2023, (1): 113-130.

[11]宋科, 徐蕾, 李振, 等. ESG投资能够促进银行创造流动性吗?——兼论经济政策不确定性的调节效应[J]. 金融研究, 2022, (2): 61-79.

[12]吴非, 胡慧芷, 林慧妍, 等. 企业数字化转型与资本市场表现——来自股票流动性的经验证据[J]. 管理世界, 2021, 37(7): 130-144,10.

[13]吴先聪, 郑国洪. 媒体关注对大股东违规减持有监督作用吗?[J]. 外国经济与管理, 2021, 43(11): 86-103.

[14]吴育辉, 张腾, 秦利宾, 等. 高管信息技术背景与企业数字化转型[J]. 经济管理, 2022, 44(12): 138-157.

[15]徐细雄, 占恒, 李万利. 党组织嵌入、政策感知与民营企业新增投资[J]. 外国经济与管理, 2020, 42(10): 3-16.

[16]张泽南, 夏玉洁, 张雪梅. 赋能还是负能: ESG表现与企业劳动投资效率[J]. 外国经济与管理, 2024, 46(7): 69-85.

[17]Amir E, Levi S, Livne T. Do firms underreport information on cyber-attacks? Evidence from capital markets[J]. Review of Accounting Studies, 2018, 23(3): 1177-1206.

[18]Angst C M, Block E S, D'Arcy J, et al. When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches[J]. MIS Quarterly, 2017, 41(3): 893-916.

[19]Bodin L D, Gordon L A, Loeb M P, et al. Cybersecurity insurance and risk-sharing[J]. Journal of Accounting and Public Policy, 2018, 37(6): 527-544.

[20]Cao X Y, Ni J, Wang F, et al. Does customer concentration affect corporate risk-taking? Evidence from China[J]. Finance Research Letters, 2023, 58: 104297.

[21]Chen J, Henry E, Jiang X. Is cybersecurity risk factor disclosure informative? Evidence from disclosures following a data breach[J]. Journal of Business Ethics, 2023, 187(1): 199-224.

[22]Chen Z F, Xie G X. ESG disclosure and financial performance: Moderating role of ESG investors[J]. International Review of

Financial Analysis, 2022, 83: 102291.
[23]Crawford S, Huang Y, Li N Z, et al. Customer concentration and public disclosure: Evidence from management earnings and sales forecasts[J]. Contemporary Accounting Research, 2020, 37(1): 131-159.
[24]D'Arcy J, Adjerid I, Angst C M, et al. Too good to be true: firm social performance and the risk of data breach[J]. Information Systems Research, 2020, 31(4): 1200-1223.
[25]Demek K C, Kaplan S E. Cybersecurity breaches and investors' interest in the firm as an investment[J]. International Journal of Accounting Information Systems, 2023, 49: 100616.
[26]Eisenkopf J, Juranek S, Walz U. Responsible investment and stock market shocks: Short - term insurance without persistence[J]. British Journal of Management, 2023, 34(3): 1420-1439.
[27]Ettredge M, Guo F, Li Y J. Trade secrets and cyber security breaches[J]. Journal of Accounting and Public Policy, 2018, 37(6): 564-585.
[28]Feng J Y, Yuan Y. Green investors and corporate ESG performance: Evidence from China[J]. Finance Research Letters, 2024, 60: 104892.
[29]Florackis C, Louca C, Michaely R, et al. Cybersecurity risk[J]. The Review of Financial Studies, 2023, 36(1): 351-407.
[30]Garcia A S, Orsato R J. Testing the institutional difference hypothesis: A study about environmental, social, governance, and financial performance[J]. Business Strategy and the Environment, 2020, 29(8): 3261-3272.
[31]Godfrey P C, Merrill C B, Hansen J M. The relationship between corporate social responsibility and shareholder value: an empirical test of the risk management hypothesis[J]. Strategic Management Journal, 2009, 30(4): 425-445.
[32]Gordon L A, Loeb M P, Sohail T. Market value of voluntary disclosures concerning information security[J]. MIS Quarterly, 2010, 34(3): 567-594.
[33]Hogarth K, Hutchinson M, Scaife W. Corporate philanthropy, reputation risk management and shareholder value: A study of Australian corporate giving[J]. Journal of Business Ethics, 2018, 151(2): 375-390.
[34]Janakiraman R, Lim J H, Rishika R. The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer[J]. Journal of marketing, 2018, 82(2): 85-105.
[35]Jeong Y C, Kim T Y. Between legitimacy and efficiency: An institutional theory of corporate giving[J]. Academy of Management Journal, 2019, 62(5): 1583-1608.
[36]Kamiya S, Kang J K, Kim J, et al. Risk management, firm reputation, and the impact of successful cyberattacks on target firms[J]. Journal of Financial Economics, 2021, 139(3): 719-749.
[37]Kasperson R E, Webler T, Ram B, et al. The social amplification of risk framework: New perspectives[J]. Risk Analysis, 2022, 42(7): 1367-1380.
[38]Lattanzio G, Ma Y. Cybersecurity risk and corporate innovation[J]. Journal of Corporate Finance, 2023, 82: 102445.
[39]Meyer J W, Rowan B. Institutionalized organizations: Formal structure as myth and ceremony[J]. American Journal of Sociology, 1977, 83(2): 340-363.
[40]Nollet J, Filis G, Mitrokostas E. Corporate social responsibility and financial performance: A non-linear and disaggregated approach[J]. Economic Modelling, 2016, 52: 400-407.
[41]Shiu Y M, Yang S L. Does engagement in corporate social responsibility provide strategic insurance-like effects?[J]. Strategic Management Journal, 2017, 38(2): 455-470.
[42]Simon F L. Global corporate philanthropy: A strategic framework[J]. International Marketing Review, 1995, 12(4): 20-37.
[43]Wang C Q, Yi J T, Kafouros M, et al. Under what institutional conditions do business groups enhance innovation performance?[J]. Journal of Business Research, 2015, 68(3): 694-702.
[44]Yang Y, Jiang Y. Buyer-supplier CSR alignment and firm performance: A contingency theory perspective[J]. Journal of Business Research, 2023, 154: 113340.
[45]Zhu W, Li W J, Wang L. The impact of environmental, social, and governance ratings on corporate innovation: From the perspective of informal institutions[J]. Managerial and Decision Economics, 2024, 45(4): 2000-2022.

Cybersecurity Risks and ESG Investments: An Explanation Based on the Reputation Insurance Mechanism

Zhang Caishi, Liu Yi

(*Antai College of Economics and Management*, *Shanghai Jiao Tong University*, *Shanghai* 200030, *China*)

Summary: Although cybersecurity has become an unavoidable risk for firms, there is limited research on how firms can prevent and respond to cybersecurity risks. Based on the reputation insurance mechanism of ESG, this paper takes China's A-share listed companies from 2010 to 2022 as the research object and empirically examines the impact and mechanism of cybersecurity risks on corporate ESG investments. The study finds that firms with higher cybersecurity risks are more likely to increase ESG investments. Lower marketization levels and higher media attention will strengthen the promoting effect of cybersecurity risks on ESG investments. Mechanism testing indicates that firms with higher cybersecurity risks can "insure" against their potential reputational risks by increasing ESG investments. Firms with greater exposure to reputational risks are more likely to increase ESG investments when faced with cybersecurity risks. Heterogeneity analysis also reveals that the positive impact of cybersecurity risks on ESG investment is more pronounced in samples with lower supply chain concentration, less managerial myopia, and a higher presence of executives with an information technology background. This paper helps understand the internal logic of firms managing cybersecurity risks through ESG investments and provides empirical evidence to encourage and guide firms to adhere to a development strategy of "technology for good".

Key words: cybersecurity risks; ESG investments; reputation insurance mechanism; marketization level; media attention

(责任编辑:王 孜)