网络安全风险治理与企业创新
——基于大语言模型的识别与发现

杨　鹏　孙伟增　田　轩　左祥太

当前，以人工智能为代表的数字技术为企业创新创造了前所未有的新机遇，同时也带来了新的风险来源：网络安全风险。根据欧洲最大的保险公司德国安联发布的《2025 安联风险晴雨表》，网络安全风险已经连续 4 年被各行业列为头号风险来源，网络攻击对企业的威胁程度甚至超过自然灾害和地缘政治冲突等传统风险。普华永道发布的《2023 年全球数字信任洞察调研中国报告》显示，全球约 65% 的受访高管计划增加企业在网络安全方面的预算支出，在中国这一比例更是高达 73%。筑牢网络安全防线、预防网络攻击并非孤立的安全议题，网络安全是国家安全的重要组成部分，是经济社会稳定运行的关键基石。对于企业而言，在数字经济时代，将网络安全风险治理嵌入创新战略中，已成为保护企业知识产权、维护国家科技安全的必要举措。

国家和企业对于现阶段亟须加强网络安全保障的广泛共识和实践，引发了学术界对网络安全风险治理问题的高度关注。与本文最为相关的文献主要关注网络安全风险对企业创新的影响，但相关结论仍存在争议。部分学者从风险对冲和技术进步的视角，认为网络安全风险会导致企业商业机密价值降低和保密成本上升，因此企业为降低对商业秘密的依赖程度和对冲数据泄露的风险，会倾向于申请更多的专利来保护知识产权。并且，网络安全风险能够倒逼企业更加重视内部网络安全防护，加大数字技术领域的研发投入力度，进而提升企业创新产出。相反地，也有学者基于创新成本视角认为，企业防范网络安全风险需投入大量资金以保障软件、硬件及网络运行安全，这会对企业的研发资金形成“挤出”效应。

现有研究尚未形成能有效指导企业网络安全治理的共识，也缺

乏从风险治理视角出发，对网络安全风险治理机制与企业创新之间关系的深入考察。本文认为，研究难点主要在于现有文献所采用的文本分析方法无法真实反映企业网络安全风险治理的复杂实践。上市企业通常会在年报中披露与网络安全相关的信息，以此向市场传达企业对网络安全风险的感知以及相关治理措施。因此，学者们大多使用词典法，以企业年报中出现的与网络安全相关的关键词数量测度企业的网络安全风险程度。然而，仅通过关键词无法直接判断企业是否开展了网络安全风险治理工作，甚至存在表意误判的问题。例如，部分企业只在年报中对全球网络安全发展趋势进行客观描述，并未谈及自身对网络安全风险的感知以及是否开展了网络安全风险治理行动。鉴于此，本文基于 2007—2021 年中国 A 股上市企业年报文本，运用大语言模型构建了衡量企业网络安全风险治理水平的指标，实证检验网络安全风险治理对企业创新的影响与内在机制。

本研究具有理论价值和现实意义。第一，本文基于大语言模型构建了一个能够反映企业真实开展网络安全风险治理的指标，克服了传统词典法无法识别企业真实行为和语义识别不准确等问题，为后续开展相关研究提供了方法参考，丰富了经济学中自然语言处理的相关文献。第二，拓展了网络安全对企业创新影响的相关研究。本文基于风险治理视角揭示了网络安全治理促进企业创新的内在机制，为现有文献中的相关争论提供了新证据，也具有政策启示意义。第三，基于溢出效应视角，考察企业网络安全风险治理对供应链上下游企业创新的影响，拓展了网络安全风险经济后果的研究视角。现有研究主要聚焦网络安全风险对企业自身经济行为和财务绩效的影响，较少讨论网络安全风险对企业供应链纵向关系的影响。本文发现企业网络安全风险治理对上游供应商和下游客户企业创新存在非对称溢出效应，丰富了数字经济背景下企业间网络风险传播与创新互动的研究框架。

本文研究发现：第一，网络安全风险治理显著提高了企业创新产出，其关键机制在于数据利用效率提升、合作创新关系稳固和融

资约束缓解；第二，该促进作用在地区网络环境较为复杂、数字技术依赖程度和国际化水平较高的企业中表现更显著，并推动企业更加重视网络安全领域的专利创造；第三，企业网络安全风险治理在供应链纵向关系中存在非对称溢出效应，对上游供应商开展网络安全创新具有正向促进作用，而对下游客户则产生反向抑制。本文研究结论表明，在数字经济时代，企业须着力提升网络安全风险治理能力，在保障网络安全的基础上实现高质量创新。

基于以上结论，为进一步提高企业网络安全风险治理水平，推动我国加快建设数字强国、创新强国，提出以下相关建议。

第一，企业应强化网络安全意识，提升风险治理能力。在善用数据与技术把握数字机遇的同时，须高度重视随之而来的安全挑战，通过完善制度与加大投入来降低风险，在保障核心数据安全的前提下稳步推进创新。供应链上游企业应主动契合客户的网络安全要求，在标准与措施上达成一致，在满足客户安全要求的同时加强自身创新能力；下游企业则可借助供应商合作获取安全保障，并加强自身网络安全能力，避免“单一依赖”。

第二，推动建立统一的网络安全治理标准，帮助企业构建系统化框架，平衡数据安全与创新发展的关系。我国已出台《中华人民共和国网络安全法》《中华人民共和国数据安全法》等法律法规，但在上市公司网络安全风险强制披露方面仍需加强。可出台专项细则，明确相关披露义务，并对接“国家信息安全漏洞共享平台”，通过定期评估，解决当前信息模糊、监管量化难等问题。

第三，政策制定中有必要考虑地区与企业差异，实施精准引导。对网络复杂地区，加强数字基础设施以提升防御能力；对高技术依赖企业，提供研发补贴或税收优惠，激励其安全技术投入与创新；对国际化企业，则积极推动网络安全标准国际对接，降低跨境贸易中的创新阻力。

《网络安全风险治理与企业创新》附录

附录 1 企业网络安全风险治理指标的统计分析

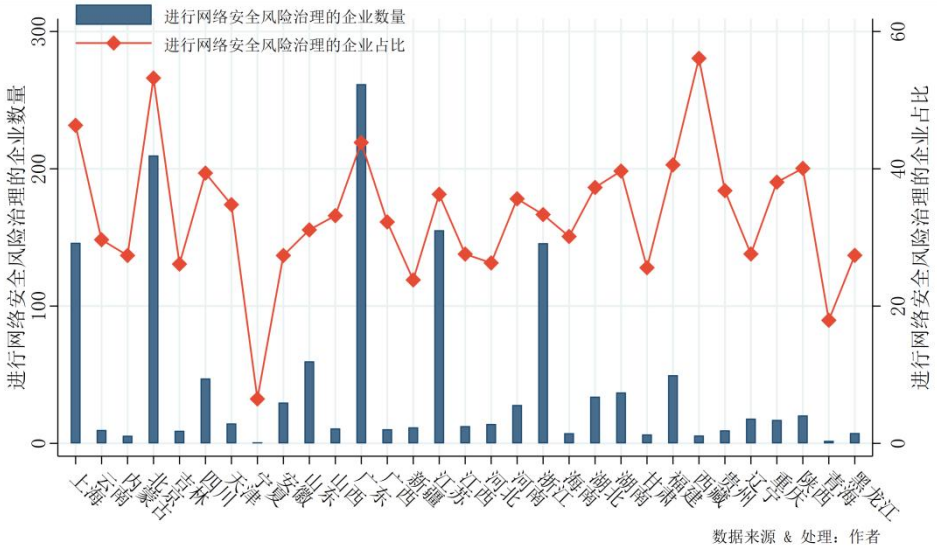
本文从时间、地区和行业三个方面，分析使用大语言模型方法构建的企业网络安全风险治理指标的趋势特征，并结合国家信息安全漏洞共享平台（CNVD）的数据进行交叉印证，以此检验本文核心指标的有效性。

第一，时间趋势。附图 1 展示了 2007—2021 年中国上市企业网络安全治理的总体趋势。2007 年，整个 A 股仅有约 15.9%的企业开展网络安全风险治理，彼时网络安全在企业经营中尚未受到广泛关注。随后，进行网络安全风险治理的企业数量呈阶梯式攀升，到 2021 年累计约有 2700 家企业针对网络安全风险实施了相应的治理措施，占比也达到 56.3%。这一变化与数字经济的发展趋势息息相关。近年来，随着我国数字经济与实体经济的融合程度不断加深，各行业的数字化转型速度加快，驱动网络安全成为企业高质量发展的基础保障。此外，伴随着近年来我国与网络安全相关的法律法规逐渐落地，要求企业作为网络运营主体必须履行安全义务，从而强化了企业的网络安全风险治理意识。未来，伴随数字技术不断更新迭代，企业会面临新的网络风险来源，为此企业必须持续提升网络安全风险治理能力，筑牢数字经济时代的安全发展屏障。

附图 1 上市企业网络安全风险治理趋势（2007—2021 年）

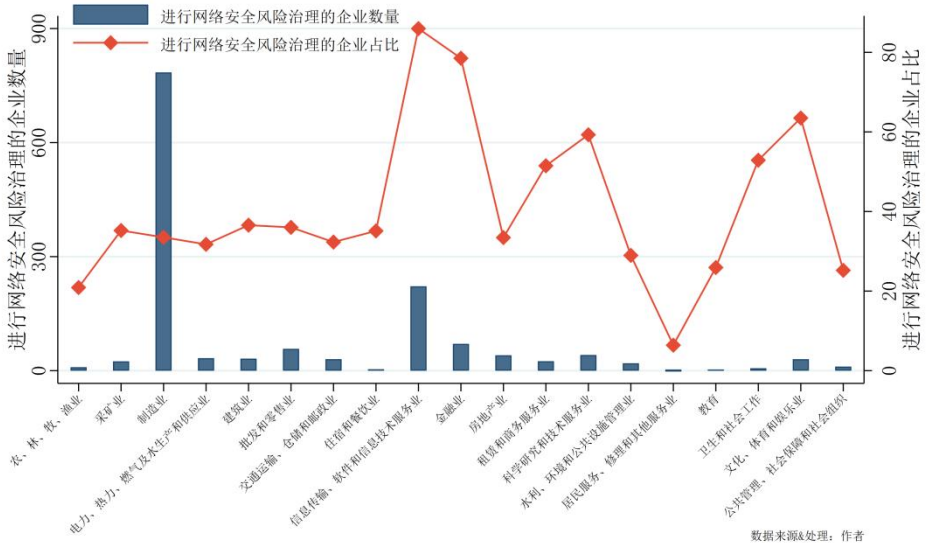
第二，地区差异。附图 2 统计了不同省份间上市企业网络安全风险治理的情况。整体来看，我国不同省份之间上市企业的网络安全治理参与度呈现出明显的“东强西弱”特征。北京、上海、江苏、浙江和广东等数字经济较发达的省份进行网络安全风险治理的企业数量和比例均较高。原因在于：一方面，这些省份的互联网、人工智能和电子商务产业较为发达，企业数字化水平较高，一旦遭遇网络威胁会直接影响企业业务正常运营，造成巨大经济损失，因此企业有动力主动开展网络安全风险治理工作。另一方面，当地政府较为重视网络安全，出台了相关的监管政策与法规要求企业落实网络安全主体责任。例如，浙江省通信管理局开展“之江数安”专项行动，全面防范网络安全风险，企业为满足制度性合法要求也会主动加强网络安全风险治理。此外，根据中国网络安全产业联盟发布的《中国网络安全产业分析报告（2023）》，京津冀、长三角和珠三角地区更加重视网络安全方面的投入，与本文的测算结果一致。相反，在数字经济相对欠发达的地区，如青海、宁夏、黑龙江等，当地上市企业的网络安全治理比例较低。这可能是因为这些地区的产业结构多以资源密集型产业为主，对

数字技术的依赖程度较低，许多企业尚未实现生产、管理和营销等环节的全面数字化，因此开展网络安全风险的动力不足。



附图 2 省份层面上市企业网络安全风险治理趋势（2007—2021 年）

第三，行业差异。根据国民经济行业分类（GB/T 4754—2017），本文计算了 2007—2021 年间每个行业进行网络安全风险治理的上市企业数量及其占比，如附图 3 所示。从绝对数量维度上看，制造业进行网络安全风险治理的企业数量庞大；农、林、牧渔业，住宿和餐饮业，居民服务、修理和其他服务业等行业，因其业务数字化复杂程度相对较低，较少在网络安全风险治理方面进行专门投入。在相对比重维度上，金融业、科学研究和技术服务业、信息传输、软件和信息技术服务业内进行网络安全风险治理的企业占比均超过了 60%，这类行业企业的日常运营高度依赖网络和信息系统，拥有大量关键数据和个人敏感信息，容易成为黑客攻击目标，因此普遍重视网络安全风险治理；文化、体育和娱乐业在数字经济时代越来越依赖网络平台进行内容创作、传播与运营，网络安全风险可能导致用户信息泄露、作品版权被盗用，因此需要通过加强网络安全风险治理维护自身合法权益；卫生和社会工作、租赁和商务服务业、交通运输和邮政业，以及电力、热力、燃气供应业等公用事业与国家安全和社会稳定密切相关，因此也较为重视网络安全风险。



附图 3 行业层面上市企业网络安全风险治理趋势（2007—2021 年）

最后，本文检索了国家信息安全漏洞共享平台（CNVD）发布的漏洞信息阅读通报数据。

2016 年 11 月以来，CNVD 每月都会对全国报送的信息安全漏洞事件进行统计与分析，并披露单位或个人报送漏洞的次数。一般而言，企业主动上报漏洞次数越多，表明企业已经建立了常态化的网络安全风险治理机制，能够及时识别自身系统中的安全缺陷。我们整理了 2016—2021 年 CNVD 披露的报送漏洞信息的企业名称，与上市公司名称进行匹配后发现，大约 13%的上市公司主动报送过漏洞信息，并且根据本文的统计，这些企业中接近 90%的企业都开展了网络安全风险治理，这也能够在一定程度上表明本文构造的指标能够准确识别企业的网络安全风险治理行为。

附录 2 主要变量定义与描述性统计

附表 1　主要变量定义与基本统计特征

变量	变量定义	均值	标准差	最小值	中位数	最大值
Innovation	企业创新水平，使用企业当年的专利申请数量衡量	23.63	64.59	0.00	3.00	473.00
CyberSecurity	企业网络安全风险治理指标，具体测度方法见正文	0.43	0.49	0.00	0.00	1.00
Age	企业年龄，经营年限（取自然对数）	2.79	0.37	1.61	2.83	3.47
Size	企业规模，总资产（取自然对数）	22.04	1.27	19.74	21.86	26.02
Lev	负债率=总负债/总资产	0.42	0.20	0.05	0.42	0.86
ROA	总资产净利润率	0.04	0.05	-0.17	0.04	0.20
Growth	营业收入增长率	0.18	0.37	-0.51	0.12	2.28
Fixed	固定资产占比=固定资产/总资产	0.22	0.16	0.00	0.19	0.71
Dual	两职合一，虚拟变量，董事长和总经理为同一人，取值为 1，否则为 0	0.26	0.44	0.00	0.00	1.00
Indenp	董事会独立性，独立董事占比	0.37	0.05	0.30	0.33	0.57
Mshare	管理层持股比例	0.13	0.20	0.00	0.00	0.70
SOE	企业所有权性质，虚拟变量，国有企业取值为 1，否则为 0	0.40	0.49	0.00	0.00	1.00

注：所有连续变量均在 1%和 99%水平上经过缩尾处理。

附录 3 其他稳健性检验

1.倾向得分匹配

考虑到不同企业之间的可观察特征变量在进行网络安全风险治理之前就可能存在显著差异，导致本文的估计结果可能有偏。对此，本文采用倾向得分匹配法来缓解样本自选择问题。具体步骤如下：第一，选取企业总资产、经营年限和所有权性质等控制变量作为协变量。第二，利用样本期内没有进行网络安全风险治理的企业构建对照组，按照 1:4 的近邻匹配原则进行匹配。第三，将匹配后的样本进行纵向合并，重新使用模型（1）进行估计。附表 2 的列（1）给出了倾向得分匹配方法得到的估计结果，可以看出，网络安全风险治理对企业专利申请的数量的影响依然在 1%的水平上显著为正，表明本文的基准结论受样本自选择的影响较小。

2.考虑企业信息披露策略[1]

年报是企业展示经营状况的重要战略性文件，年报的内容通常划分为当前经营状况回顾和未来发展展望两个部分，其中“当前经营状况回顾”部分更能够体现企业的实际行动。本文参考彭俞超等（2023）的做法，将企业网络安全风险治理指标划分为“实际行动型”（*CSactual*）和“未来计划型”（*CSplan*）。其中，“实际行动型”是指企业在年报的当前经营状况回顾部分提到的已完成的网络安全风险治理行动；“未来计划型”是指企业在年报的

1 感谢审稿人的建议。

未来发展展望部分披露的未来可能开展的网络安全风险治理计划。附表 2 列（2）、（3）展示的结果显示，*CSactual* 的回归系数在 5%的统计水平上显著，但是 *CSplan* 的系数较小且不显著。这一发现表明，企业网络安全风险治理效果的有效性主要来源于其已落实的实际行动，而非对未来的计划。企业在年报中关于未来网络安全建设的展望，若缺乏后续可执行的具体方案，将不能切实提升企业实际的网络安全治理能力。

3.遗漏变量

研发投入向来是影响企业创新产出的关键要素。本文的核心被解释变量——专利数量，是企业研发投入活动的直接产出。已有大量文献证实了研发投入与创新产出之间存在显著的正向关系，为此本文进一步在基准模型（1）中控制取对数的企业研发投入金额（*RD*），以避免遗漏变量偏误。需要说明的是，根据本文的统计，2012 年之前约有 40%的样本企业并未披露研发投入数据。由于本文的样本期间为 2007—2021 年，因此，为了避免回归样本大量缺失，本文并未在基准回归中控制研发投入这一指标。回归结果见附表 2 列（4），可以看出，在考虑遗漏变量问题后，企业网络安全风险治理变量的回归系数依然在 1%的水平上显著为正，表明本文的结论是稳健的。

4.调整解释变量

本文基准回归主要使用百度公司开发的 ERNIE 大模型构造核心解释变量，为了增强结果的稳定性，同时考虑到模型开发的成本，我们进一步选择杭州深度求索公司开发的 DeepSeek 大模型对标注准确率进行了重分类验证，重新构造企业网络安全治理指标。具体步骤如下：第一，从初始语料库中随机筛选部分观测样本进行重分类验证。由于 DeepSeek 对文件规模具有读取上限，我们无法将语料库中所有的文本都输入 DeepSeek 客户端进行分类处理。第二，将筛选后的样本按照 6:4 进行划分，60%的样本作为训练集（保留标注），40%的样本作为测试集（隐匿标注）。第三，将 60%的样本与其真实标签输入给 DeepSeek 进行特征学习。第四，让 DeepSeek 根据学习结果对剩下 40%的样本进行基于 LLM 的标注。第五，比较 LLM 的标注结果与人工标注结果（真实标签）的差异性，结果发现，DeepSeek 对测试集样本标注的正确比例约为 87.24%，略小于本文所使用模型的正确率。最后，我们将基于 DeepSeek 大模型构造的企业网络安全治理指标记为 *CSdeepseek*，重新带入基准模型后的回归结果如附表 2 列（5）所示，*CSdeepseek* 的回归系数在 5%的统计水平上显著为正，验证了本文研究结论的稳健性。

5.调整被解释变量

在基准回归中，本文主要从创新数量的角度考察网络安全风险治理对企业创新的影响，但是我国技术创新存在创新数量不断上升、质量相对落后的问题。因此，本文进一步从创新质量的角度重新构造被解释变量：第一，发明专利的申请数量（*PatInv*）。根据中国专利法第二条规定，专利可以被划分为发明、实用新型和外观设计三种类型，其中，发明专利的技术含量最高且申请难度最大，能够在一定程度上代表企业的创新质量。第二，使用企业获得授权专利的被引用次数衡量企业的创新产出质量。特别地，Boeing and Mueller（2019）指出中国的专利存在大量的自引用现象，这可能导致企业的创新质量被高估。基于此，本文在剔除了企业专利自引用的次数，仅使用他引次数衡量企业创新质量，记为 *PatCited*。回归结果见附表 2 列（6）、（7），可以看出，网络安全风险治理对企业发明专利申请数量和授权专利被引用次数（去除自引）的影响分别在 1%和 5%的水平上正向显著，表明网络安全风险治理有利于提升企业的创新质量。

6.排除特殊样本干扰

与传统行业相比，网络安全行业的企业拥有更强的网络安全风险治理能力，并且能够为其他企业提供网络安全产品与服务。根据《中国网络安全产业分析报告（2023）》的数据统计，截至 2023 年 6 月，中国公开上市的网络安全企业共计 26 家，其中，奇安信、启明星辰

和深信服三家企业在国内网络安全产品的市场占有率均超过了 6%。因此，回归中包含网络安全行业样本可能会导致本文的估计结果存在高估的情况。为此，本文将网络安全企业样本剔除，重新进行回归。估计结果如附表 2 列（8）所示，在剔除网络安全企业样本后，本文的基准结论依然成立。

附表 2　其他稳健性检验

	倾向得分匹配	考虑企业信息披露策略		遗漏变量	调整解释变量	调整被解释变量		排除特殊样本
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	Innovation	*Innovation*	*Innovation*	*Innovation*	*Innovation*	*PatInv*	*PatCited*	*Innovation*
CyberSecurity	0.1343***			0.1396***				
	(2.7451)			(3.5764)				
CSactual		0.1464**						
		(2.5075)						
CSplan			0.0461					
			(1.3892)					
RD				0.1445***		0.1605***	0.1390**	0.1396***
				(4.3997)		(2.7209)	(1.9993)	(2.9395)
CSdeepseek					0.1385***			
					(2.8978)			
控制变量	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
企业固定效应	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
城市×年份固定效应	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
样本量	30616	30715	30715	30715	30715	30715	30715	30611
Pseudo R^2	0.8422	0.8419	0.8417	0.8431	0.8420	0.8104	0.9076	0.8420

注：括号内为 *z* 值，采用行业层面的聚类异方差稳健标注误进行估计；***、** 和 * 分别表示在 1%、5% 和 10%的水平上显著，下表同。

附录 4 差异化分析

1.地区网络环境复杂度

在复杂的网络环境中，网络安全风险治理能够帮助企业防范日益变化的计算机病毒和检查可能存在的安全漏洞，在保证企业核心数据安全性的基础上实现创新活动的连续性和稳定性。此外，复杂的网络环境也倒逼企业必须通过数字技术手段加强网络安全风险治理能力，有利于企业开发新的数字化产品与服务。因此，一个合理的推测是，在网络环境复杂度较高的地区，网络安全风险治理更有利于促进企业创新。

本文使用企业所在省份的域名数量衡量地区网络环境的复杂程度。一般而言，地区的域名数量越多，意味着当地网络环境的复杂度较高。因为随着域名的增多，地区内部的网络空间更为丰富，网站、应用、服务之间的联系多样化，但是潜在的网络安全威胁也随之增加，如域名劫持、虚假网站等问题。域名数量数据来源于历年的中国统计年鉴，本文根据该指标的中位数对样本进行分组。附表 3 列（1）、（2）汇报的分组回归结果表明，在域名数量较多，即网络环境较为复杂的地区，网络安全风险治理对企业创新的提升作用更强。

2.企业数字技术依赖程度

Florackis et al.（2023）指出企业对数字技术的依赖程度越高，受到网络攻击的负面影响反而会更强。例如，软件开发、电子商务和互联网服务等行业的企业在日常经营过程中都较为依赖数字技术的稳定运行，这类企业会更加重视网络安全和数据保护，这种持续的网络安全需求激励企业不断创新，以保持对不断演变的网络安全威胁问题的应对能力。基于此，本文认为，网络安全风险治理对数字技术依赖程度较高的企业可能具有更强的创新激励效果。

参考金星晔等（2024），本文运用大语言模型，从企业年报爬取与数字技术相关的语句数量，以此作为企业数字技术依赖度的代理变量。一般而言，企业在年报中提到与数字技术相关的信息越多，那么企业对数字技术的依赖程度可能越高。按照词频的中位数将样本划分

为数字技术依赖程度高和低两组，分样本回归结果见附表 3 列（3）、（4）。可以看出，网络安全风险治理仅对数字技术依赖程度较高的企业具有显著的创新激励作用。

3.企业国际化程度

自从中国加入世界贸易组织以来，越来越多的企业将业务开拓到国际市场，并在海外设立分公司，这在提升企业国际化的同时也扩大了企业的网络边界，导致企业遭受网络攻击的可能性提升。根据《2023 年全球高级持续性威胁研究报告》，2023 年南亚和中东等地区的黑客组织针对中国驻外企业的网络攻击活跃度明显上升。原因在于海外业务通常涉及大量跨国数据传输，包括客户信息、业务合同、财务数据等，企业必须加强网络安全风险治理能力来保证数据传输的保密性和安全性。并且，不同国家的数据中心和网络安全服务在技术能力可能存在差异，导致部分节点容易成为黑客攻击突破口。例如，某上市企业 2018 年的年报中提到“集团的大部分销售是通过世界各地的子公司开展，遍布全球市场”，并且“集团在开展经营活动时可能面临与其信息技术系统稳定性、数据保护和网络相关的风险和威胁……为了最大限度地降低上述风险，集团也投入资源加强自身技术力量，并恰当保护自身系统。”因此，本文预期，对于国际化程度更高的企业而言，网络安全风险治理对企业创新的激励作用更为明显。

参考陈立敏等（2016），本文使用企业海外营业收入占总营业收入的比重测度企业的国际化程度，并根据指标的中位数将样本划分为高低两组。分样本回归结果如附表 3 列（5）、（6）所示，结果发现，在国际化程度较高的样本中，网络安全风险对企业创新的影响在 1%的水平上显著为正，但在国际化程度较低的样本中，上述影响并不显著，与前文预期一致。

4.区分专利技术领域

为了应对不断演变的网络安全威胁（如计算机病毒、黑客攻击和软件漏洞等），企业可能会通过引入云计算、物联网和区块链等技术来提升信息系统的安全性，在加强数据安全和降低网络安全风险的同时，可能会推动企业加大对网络安全技术领域的投资和研发力度。Gomes et al.（2023）使用美国上市企业的数据发现，关于网络安全保护的需求推动企业更加追求网络安全技术领域的创新，尤其对金融、医疗和软件等数据密集型企业影响更加明显。

本文参考 Gomes et al.（2023）的方法，在专利分类号的小组层面识别出与网络安全技术领域相关的专利。例如，专利分类号为 G06F21/60 属于数据安全领域，特指通过技术手段确保数据在存储、传输或处理过程中不被篡改、破坏或未经授权修改。据此，本文将企业当年申请的专利数量划分为网络安全专利（*CyberPat*）和非网络安全专利（*NoCyberPat*），分别代入模型（1）重新进行回归。回归结果见表 10 的列（7）、（8），可以看出，网络安全风险治理对企业在网络安全专利和非网络安全专利的影响均在 1%的水平上显著为正，这表明网络安全风险治理对企业创新的影响不是仅仅限于网络安全技术本身，而是对于企业的生产活动具有广泛的创新促进作用。进一步比较解释变量系数的大小发现，相较于非网络安全专利，网络安全风险治理对网络安全专利的影响更强。这意味着，网络安全风险治理过程直接引发了企业对网络安全技术创新的重视。

附表 3 差异化分析

	(1) *Innovation* 网络环境复杂度高	(2) *Innovation* 网络环境复杂度低	(3) *Innovation* 数字技术依赖度高	(4) *Innovation* 数字技术依赖度低	(5) *Innovation* 国际化程度高	(6) *Innovation* 国际化程度低	(7) *CyberPat* 网络安全专利	(8) *NoCyberPat* 非网络安全专利
CyberSecurity	0.1649**	0.0809	0.1103***	0.1210	0.1527**	0.0729	0.6907***	0.1368***
	(2.4268)	(1.5630)	(2.7985)	(1.6424)	(2.5001)	(0.9651)	(8.7792)	(2.8431)
控制变量	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
企业固定效应	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
城市×年份固定效应	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
样本量	15352	15363	14338	16377	15357	15358	30715	30715
Pseudo R^2	0.8589	0.8514	0.8617	0.8576	0.8584	0.8302	0.6392	0.8397

附录参考文献

[1] 陈立敏、刘静雅和张世蕾，2016，《模仿同构对企业国际化—绩效关系的影响——基于制度理论正当性视角的实证研究》，《中国工业经济》第 9 期，第 127~143 页。

[2] 彭俞超、王南萱和顾雷雷，2023，《企业数字化转型、预判性信息披露与股价暴跌风险》，《财贸经济》第 44 卷第 5 期，第 73~90 页。

[3] Boeing, P. and E. Mueller, 2019, “Measuring China’s Patent Quality: Development and Validation of ISR Indices,” *China Economic Review*, 57, p. 101331.

[4] Gomes, O., R. Mihet, and K. Rishabh, 2023, “Data Risk, Firm Growth, and Innovation,” *Swiss Finance Institute Research Paper*, No. 23-86.

[5] Florackis, C., C. Louca, R. Michaely, and M. Weber, 2023, “Cybersecurity Risk,” *The Review of Financial Studies*, 36(1), pp. 351~407.