网络安全治理与股价崩盘风险
——基于上市公司年报文本分析的证据

作者简介：

王辉，教授，理学博士，博士生导师，教育部新世纪优秀人才，北京市青年英才，中央财经大学金融学院党委书记，北京市海淀区学院南路 39 号，电话：18515218230，邮箱：xiaohuipk@163.com

何冬昕（通讯作者），博士研究生，中央财经大学金融学院，北京市昌平区中央财经大学（沙河校区），电话：18510204497，邮箱：lflovert@sina.com

陈旭，副研究员，经济学博士，中国财政科学研究院金融研究中心，北京市海淀区阜成路甲 28 号，电话 13021142698，邮箱：allanchen100@163.com

姜富伟，教授，金融学博士，博士生导师，教育部青年长江学者，中央财经大学金融学院金融工程系主任，北京市海淀区学院南路 39 号，电话：18511086494，邮箱：jfuwei@gmail.com

邮寄地址：北京市昌平区沙河高教园-中央财经大学 3 号学院楼

摘要：网络安全治理已经引起了政府决策部门和学术界的广泛关注。本文聚焦资本市场中的企业网络安全治理与金融风险，通过深度学习方法分析上市公司年报文本，构建企业网络安全治理指标，实证研究揭示了网络安全治理和股价崩盘风险之间的关系及其机制。研究发现，网络安全治理可以显著降低股价崩盘风险，这一结论在更换解释变量、增加控制变量和《网络安全法》的颁布作为准自然实验等稳健性检验后仍然成立。企业网络安全治理降低了外界的信息不对称、增加了企业社会责任，从而降低了股价崩盘风险。国有企业、规模较大、公司成长性较好、有形资产比例较低的公司更有可能重视网络安全治理。本文结论为企业网络安全治理对金融风险的影响提供了经验证据，为企业网络安全治理相关政策制定提供了建议参考。

关键词：股价崩盘风险；网络安全治理；文本分析；信息不对称；企业社会责任

Governance of Cybersecurity and Stock Price Crash Risk: Evidence from Textual Analysis of Chinese Listed Firms' Annual

Reports

Wang Hui [1] He Dongxin [1] Chen Xu [2] Jiang Fuwei [1]

[1] School of Finance，Central University of Finance and Economics

[2] Research Center for Finance，Chinese Academy of Fiscal Sciences

Abstract: The issue of cybersecurity governance has gained wide attention from government decision-making departments and academia. This paper focuses on the cybersecurity governance of enterprises in capital markets and its relationship with financial risk. By employing deep learning methods to analyze the text of annual reports of listed companies, this study constructs indicators for enterprise cybersecurity governance. Through empirical research, it reveals the relationship and mechanism between cybersecurity governance and stock price crash risk. The study finds that cybersecurity governance can significantly reduce stock price crash risk, and this conclusion remains robust even after conducting sensitivity tests by changing explanatory variables, adding control variables, and treating the promulgation of "Cybersecurity Law" as a quasi-natural experiment. By reducing information asymmetry and increasing corporate social responsibility, enterprise cybersecurity governance lowers stock price crash risk. State-owned enterprises, larger firms, those with higher growth potential, and those with lower proportions of tangible assets are more likely to prioritize cybersecurity governance. The findings of this paper provide empirical evidence on the impact of enterprise cybersecurity governance on financial risk and offer policy recommendations for the development of relevant policies on enterprise cybersecurity governance.

Key words: Stock price crash risk , Cybersecurity governance , Textual analysis ， Asymmetric information ， corporate social responsibility

中图分类号：F832　　文献标识码：A

*本研究得到教育部哲学社会科学研究重大课题攻关项目《平台资本垄断视角下金融风险防控研究》（22JZD011）、国家自然科学基金资助项目《基于异质性关联网络的系统性风险演化机制与防范化解研究》（72273165）、国家社会科学基金重大项目《负利率时代金融系统性风险的识别和防范研究》（20&ZD101）的资助，特此感谢。何冬昕为本文通讯作者。

网络安全治理与股价崩盘风险
——基于上市公司年报文本分析的证据

王辉　何冬昕　陈旭　姜富伟

摘要：网络安全治理已经引起了政府决策部门和学术界的广泛关注。本文聚焦资本市场中的企业网络安全治理与金融风险，通过深度学习方法分析上市公司年报文本，构建企业网络安全治理指标，实证研究揭示了网络安全治理和股价崩盘风险之间的关系及其机制。研究发现，网络安全治理可以显著降低股价崩盘风险，这一结论在更换解释变量、增加控制变量和《网络安全法》的颁布作为准自然实验等稳健性检验后仍然成立。企业网络安全治理降低了外界的信息不对称、增加了企业社会责任，从而降低了股价崩盘风险。国有企业、规模较大、公司成长性较好、有形资产比例较低的公司更有可能重视网络安全治理。本文结论为企业网络安全治理对金融风险的影响提供了经验证据，为企业网络安全治理相关政策制定提供了建议参考。

关键词：股价崩盘风险；网络安全治理；文本分析；信息不对称；企业社会责任

一、引言

近年来，网络安全风险已经成为影响我国经济安全的重要风险之一。网络信息系统作为数字经济发展的重要载体，其安全问题是我国经济高质量发展面临的重大挑战。新冠疫情的影响使得经济活动对互联网的依赖性更强，叠加大国博弈与地缘政治等因素，使得网络攻击日益常态化、频繁化、国际化。企业部门是网络安全风险的重灾区，网络安全事件除了导致企业系统服务中断或数据泄露造成直接的经济损失外，还会因此衍生信任危机与法律风险（Steinbart et al.，2013）。在资本市场上，企业受到网络攻击后衍生的信任危机与法律风险会导致企业股价大幅下降，造成金融风险，影响国家金融安全（王秦、朱建明，2018），例如，2018 年 8 月 28 日，华住酒店发生用户信息泄露事件，泄露用户敏感信息近 5 亿条，当日华住股价大跌超过 5%。

以习近平同志为核心的党中央高度重视网络安全风险问题。早在 2016 年 4 月的网络安全和信息化工作座谈会上，习近平总书记就强调指出，要树立正确的网络安全观，增强网络安全防御能力和威慑能力。在 2018 年 4 月的全国网络安全和信息化工作会议上，习近平总书记再次强调，“没有网络安全就没有国家安全”，“要落实关键信息基础设施防护责任，行业、企业作为关键信息基础设施运营者承担主体防护责任，主管部门履行好监管责任。”党的二十大报告进一步强调健全国家安全

体系，指出要“强化经济、重大基础设施、金融、网络、数据、生物、资源、核、太空、海洋等安全保障体系建设”。

网络安全风险治理问题是数字经济时代的重要课题，同时，网络安全治理也是公司治理的重要组成部分（胡晓明等, 2014）。目前，关于企业网络安全对金融市场影响的研究，主要包括以下两个方面：一是侧重于企业网络安全风险造成的经济后果研究。目前的研究主要从数据泄露事件、信息服务停止事件等不同的网络安全事件对企业声誉、法律风险、资本权益、企业现金流、融资约束、溢出效应造成的不同影响等方面展开探究（王秦、朱建明，2018；尚兆燕、刘凯扬，2019；Kwon et al.，2013；Deng et al.，2021；Eisenbach et al.，2022；Steinbart et al.，2013；Kamiya et al.，2021）。二是侧重于从企业网络安全风险管理角度进行研究。主要研究了如下问题：具有技术背景的高管特征对企业网络安全治理的影响，企业产权性质、股权结构、内部审计能力异质性对企业网络安全治理的影响等（Vincent et al.，2017；Steinbart et al.，2013；甄杰等，2020）。

目前对网络安全治理与金融市场稳定的研究主要是从宏观层面出发运用理论分析探讨网络安全的治理策略，鲜有文献从微观企业视角研究企业的网络安全治理对金融风险的影响问题。股价崩盘风险是金融风险的重要一环（彭俞超等，2018），降低股价崩盘风险是维护金融市场稳定的重要任务，本文尝试对这一问题进行探究，以网络安全治理信息披露对股价崩盘风险的影响作为切入点，深入讨论网络安全治理对金融市场稳定的影响。

为探究企业网络安全治理与股价崩盘风险的关系，本文提出如下问题：企业网络安全治理情况在上市公司中披露程度如何？企业网络安全治理信息披露如何影响股价崩盘风险？其背后的影响机制是什么？上述影响在不同的公司间是否存在着异质性？什么因素影响企业关注网络安全治理？对上述问题的回答，从短期来看，有助于为中国上市公司股价崩盘风险研究提供新视角、新思路；从长期来看，有助于在数字经济快速发展和网络安全形势日益严峻的大环境下，为中国加强网络安全治理、维护金融市场稳定提供实证支撑。

为了解决上述问题，本文基于2006—2019年间中国A股上市公司样本，通过人工筛选获取“网络安全治理”种子词，将上市公司年报文本通过jieba分词与Word2vec深度学习技术对12亿词语的年报文本语料库进行词向量生成训练，得到基于年报文本的词向量模型。通过“网络安全治理”种子词和词向量模型，计算并生成“网络安全治理”扩展词，将“网络安全治理”种子词与扩展词相加，合成“网络安全治理”相关词词典。通过该词典在上市企业年报文本中获取与“网络安全治理”相关的关键词，构造上市企业“网络安全治理”的衡量指标，并进一步研究上市企业网络安全治理对股价崩盘风险的影响。研究发现，网络安全治理可以显著降低股价崩盘风险，这一结论在更换解释变量、增加控制变量和《网络安全法》的颁布作为准自然实验等稳健性检验后仍然成立。企业网

络安全治理降低了外界的信息不对称、增加了企业社会责任，从而降低了股价崩盘风险。国有企业、规模较大、公司成长性较好、有形资产比例较低的公司更有可能重视网络安全治理。

综上，本文的研究贡献主要体现在以下几个方面：第一，使用基于 Word2vec 深度学习技术和自然语言处理技术，利用非结构化的企业年报文本数据构造了中文语境下网络安全治理关键词，测度网络安全风险治理情况指标，并为后续研究提供了扎实的数据基础；第二，实证检验了企业网络安全治理对降低股价崩盘风险的积极意义，深入探索了其影响机制，丰富股价崩盘风险影响因素的相关研究，为网络安全治理对于维护国家金融稳定的作用提供了实证证据。第三，通过网络安全治理对股价崩盘风险的异质性研究，发现规模不同、产权性质不同公司的网络安全治理对股价崩盘风险的影响存在差异，为监管部门制定具有针对性的网络安全治理政策提供了参考。第四，基于本文的研究成果，基于中国企业现实数据，充分结合中国网络安全治理的发展现状与相关政策，提出了我国网络安全治理与风险防范的政策建议。

二、文献回顾

（一）上市公司网络安全治理

关于公司网络安全治理的研究主要从影响公司网络安全治理的因素角度入手，探究公司网络安全治理差异的原因。经理人和董事会的特征对企业网络安全治理至关重要，当公司高管具有 IT 相关从业经历（Kwon et al.，2013）或者公司 CIO 管理层地位较高时（Vincent et al.，2017），企业的网络安全治理能力会加强。当 CIO 有较高风险规避倾向时，更容易减少公司网络安全风险事件带来的损失（Feng and Wang，2019）。Nordlund（2021）发现董事会成员具有较高网络安全知识水平以及成员性别的多元化时，会加强网络安全信息披露。此外，外部监管要求变化会影响企业网络安全治理结构及相关信息披露的策略。《萨班斯-奥克斯利法案》（Sarbanes-Oxley Act，SOX）促进了企业的网络安全信息披露（Gordon et al.，2006）；泄露信息披露法促进了企业加强网络安全管理，则企业数据泄露事件会减少（Ashraf and Sunder，2020）。在国内的研究中，甄杰等（2020）发现公司高管增加对公司网络安全绩效的考核，会增加企业绩效；林润辉等（2016）发现信息安全监管政策可以促进企业加强网络安全制度内化，提高企业竞争力和绩效。

目前，关于中国企业网络安全治理的研究相对较少，本文拟从网络安全治理信息披露的角度探究如下两个问题：中国上市企业网络安全治理情况在上市公司中披露程度如何？什么因素影响企业关注网络安全治理？企业网络安全治理的指标刻画是研究上述问题的关键，企业网络安全治理信息在传统的结构化数据中很难刻画，上市公司披露的财务信息中不包含企业网络安全治理相关数据。

在以往的研究中，对于企业网络安全治理的指标刻画主要以问卷调研为主，问卷调研存在调研范围较小和问卷本身设计缺陷，可能导致选择性偏误。

本文采用基于上市公司年报文本的非结构化文本数据对企业网络安全治理指标进行测度，上市公司年报文本直接反映了上市公司对于网络安全的重视程度与信息披露程度。本文通过使用从公司年报的文本信息中抓取与“网络安全治理”相关的关键词，构造网络安全治理的衡量指标。目前国内关于网络安全治理的文本研究相对较少，在美国市场的研究中，Florakis et al.（2020）与 Jamilov et al.（2021）通过人工筛选的网络安全相关词对美股 10-K 年报文本与电话会议文本中“网络安全”关键词的出现频次对网络安全事项进行刻画。但该方法主要研究美股市场，文本为英语语境，本文的研究主题是中国 A 股中文年报，目前国内的研究中尚未有针对网络安全事项构建的现有中文词典。此外，美国证券交易委员会 2011 年后在管理条例 S-K 第 305 项中规定：公司必须在其财报——第 1A 项“风险因素”中提供有关网络安全风险如何影响其运营的信息，特别是重大网络安全风险和事件。但我国证券市场管理机构并未强制要求公司在年报文本中披露其网络安全风险与管理情况。这使得在中国 A 股年报中对网络安全治理信息的披露远不及美股 10-K 年报，导致使用人工筛选的关键词挖掘方法在年报中出现的频率较低，涉及的上市公司较少，不利于本文研究问题所需信息的挖掘。

为解决上述问题，本文使用参考 Li et al.（2021）的方法，将上市公司年报文本通过 jieba 分词与 Word2vec 深度学习技术对年报文本进行词向量生成，得到基于年报文本的词向量模型（Word Embedding）。通过“网络安全治理”种子词和词向量模型，计算并生成“网络安全治理”扩展词。然后将“网络安全治理”种子词与扩展词相加，合成“网络安全治理”相关词词典，通过该词典从上市企业年报文本中获取与“网络安全治理”相关的关键词，构造上市企业“网络安全治理”的衡量指标。

（二）股价崩盘风险

关于股价崩盘风险产生的实证研究，通常在委托代理理论框架下讨论，企业经理人有能力和动机隐藏公司的负面消息，当隐藏的负面消息累积达到一定上限的时候，负面消息已无法被隐藏从而形成了股价大幅下跌的股价崩盘风险（Jin and Myers，2006；Hutton et al.，2009）。

现有文献证明投资人与企业信息不对称是股价崩盘风险的重要渠道，企业信息透明度是影响股价崩盘风险的重要因素（卞世博等，2022）。企业经理人因其声誉、薪酬绩效、生涯履历、内部晋升等原因有能力和动机隐藏公司的负面消息（Graham et al.，2005；Kothari et al.，2009；Piotroski et al.，2015）。同时，企业经理人隐藏负面消息的手段也有所不同，如企业避税、企业过度投资、操纵媒体信息、股权质押等（江轩宇、许年行，2015；李文贵、路军，2022；Kim et al.，2011；谢德

仁等，2016）。因此，约束经理人隐藏负面消息的治理机制对降低股价崩盘风险有着显著作用，如外部监督机制、内部治理机制、增加企业社会责任与企业信任等（Callen and Fang，2013；权小锋等，2015；叶康涛等，2015；Li et al.，2017）。

本文认为，网络安全治理是企业治理的一部分。相比于财务信息等信息，企业治理、公司发展规划等信息往往更难获取与理解，但对投资人的投资决策也同样具有重要的影响（Coval and Moskowitz，1999）。企业披露网络安全治理相关信息，可能从以下两个维度影响股价崩盘风险，一方面可以帮助投资人理解企业的治理情况，加强外部监督机制，提高信息的准确性与信息质量（赵静等，2018），另一方面，网络安全治理作为企业社会责任的一部分，企业重视网络安全治理可以提高企业社会责任，提振投资人信心（黄金波等，2022）。

三、网络安全治理指标测度

（一）网络安全治理词典构建的整体方法

本文利用年报文本与 word2vec 深度学习方法构建网络安全治理词典并计算相关指标，具体流程如图 1 所示。本文的一个核心解释变量是“某年某家上市公司是否披露了网络安全治理事项”，但上市公司的网络安全治理水平作为公司治理的内容，在公开数据集中很难找到直接反应这一情况的相关指标。为了尽可能刻画公司网络安全治理的情况，并且尽可能覆盖中国 A 股所有上市公司样本，本文提出的一种网络安全风险的衡量方式：基于上市公司披露的年报文本信息，通过 jieba 工具对于年报文本进行分词，获得 A 股年报文本语料库。对 A 股年报文本语料库使用 word2vec 方法训练中文年报文本词向量模型，使用词向量模型计算与“网络安全治理种子词”语义相近的“网络安全治理扩展词”并构成“扩展词典”，将种子词典与扩展词典合并获得“网络安全治理词典”。

该方法与传统词典-词频文本方法不同的是，本文使用的一种基于 Word2Vec 深度学习方法的关键词扩展方法增强测度指标的准确性。该方法主要分为两步：第一步，利用前向神经网络将所有出现在年报文本中的词语（即语料库）处理成为一个具有固定维度的向量（即进行 word2vec 词嵌入处理）；第二步，利用所有词的向量与种子词向量做余弦相似度分析，把最为相似的生成为扩展词，并与种子词合并构成词典。该方法在 Li et al.（2021）与姜富伟等（2021）的研究中也有使用。

采用深度学习方法扩展词典的原因是人工筛选关键词时往往存在两类偏误：第一类偏误是，关键词词库的获取往往通过过往的经验文本进行获取，如从相关主题的各类报告、文献中人工筛选关键词，这会导致一部分在经验文本中提及的关键词从未在年报文本中提及；第二类偏误是，从经验文本中筛选的关键词无法覆盖年报文本中全部表示该类含义的关键词，可能遗漏关键词，最终导致

结果出现误差。

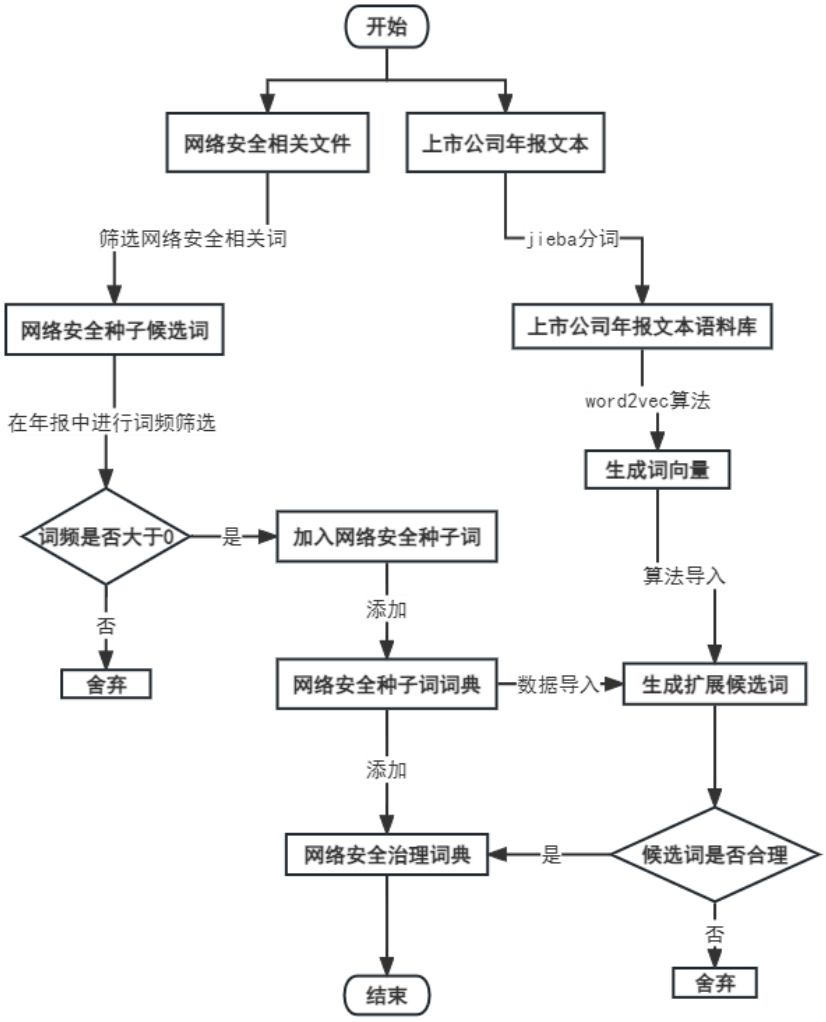


图1　网络安全治理词典构建流程

（二）网络安全治理种子词典的构建

本文的网络安全治理种子词的选取主要依托于《中华人民共和国网络安全法》《中华人民共和国数据安全法》《关键信息基础设施安全保护条例》等法律法规文件与《网络安全审查办法》《云计算服务安全评估办法》《2020年我国互联网安全态势综述》《中国互联网网络安全报告》《全球网络安全政策法律发展年度报告》等研究报告文件，选取如下5个包含了企业网络治理不同维度的关键词：（1）网络安全风险披露；（2）网络安全防护；（3）网络安全攻击类型；（4）网络安全专用设备；（5）网络安全事件后果。在此基础上，将人工筛选出的关键词在年报文本中进行词频统计，剔除了词频为“0”的关键词，因为这意味着在年报文本中未曾出现，属于不相关词语。基于此，我们

筛选了网络安全治理种子词词典，如表1所示。

表1　　网络安全治理种子词、频次及定义

网络安全治理种子词典		
关键词	**频次**	**定义**
网络安全	7605	指网络系统的硬件、软件及其系统中的信息受到保护。它包括系统连续、可靠、正常地运行，网络服务不中断，系统中的信息不因偶然的或恶意的行为而遭到破坏、更改或泄露。
网络攻击	222	指针对计算机信息系统、基础设施、计算机网络或个人计算机设备的任何类型的进攻动作。
数据泄露	110	指敏感的、受保护的或机密的数据有可能被一个未经授权的组织剽窃、盗走或使用。
系统漏洞	36	指应用软件或操作系统软件在逻辑设计上的缺陷或错误，被不法者利用，通过网络植入木马、病毒等方式来攻击或控制整个电脑，窃取其中的重要资料和信息，或者破坏系统。
计算机病毒	126	指编制者在计算机程序中插入的破坏计算机的功能或者数据，影响其正常使用并且能够自我复制的一组计算机指令或程序代码。
数据安全	2230	指为数据处理系统建立和采用的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因遭到破坏、更改和泄露。
拒绝服务	74	指通过向服务器发送大量垃圾信息或干扰信息的方式，导致服务器无法向正常用户提供服务的现象。
访问控制	196	指防止对任何资源进行未授权的访问，从而使计算机系统在合法的范围内使用。

（三）Word2Vec算法与词向量模型

在获取种子词的基础上，进一步使用word2vec算法从年报文本中训练词向量并计算词语相似度，从而提取与网络安全治理种子词的相关词语，在此基础上挑选具有合适表示网络攻击治理的词语作为扩展词并达到扩展词典的目的。

Word2vec算法是Mikolov et al.（2013）提出的一种深度学习词向量模型，该模型可以通过训练把文本内容处理为高维度的向量表示，而向量空间上的余弦相似度可以用来表示文本语义上的相似度。Word2vec模型主要包括CBOW模型与Skip-gram模型2种训练模型，CBOW模型通过上下文预测

当前词，而Skip-gram模型则通过当前词预测上下文，如图2所示。因为本文是通过“网络安全治理种子词”发现“新词”从而扩展词库，词典中存在一些低频率的词语，本文应用Skip-gram模型进行估计。

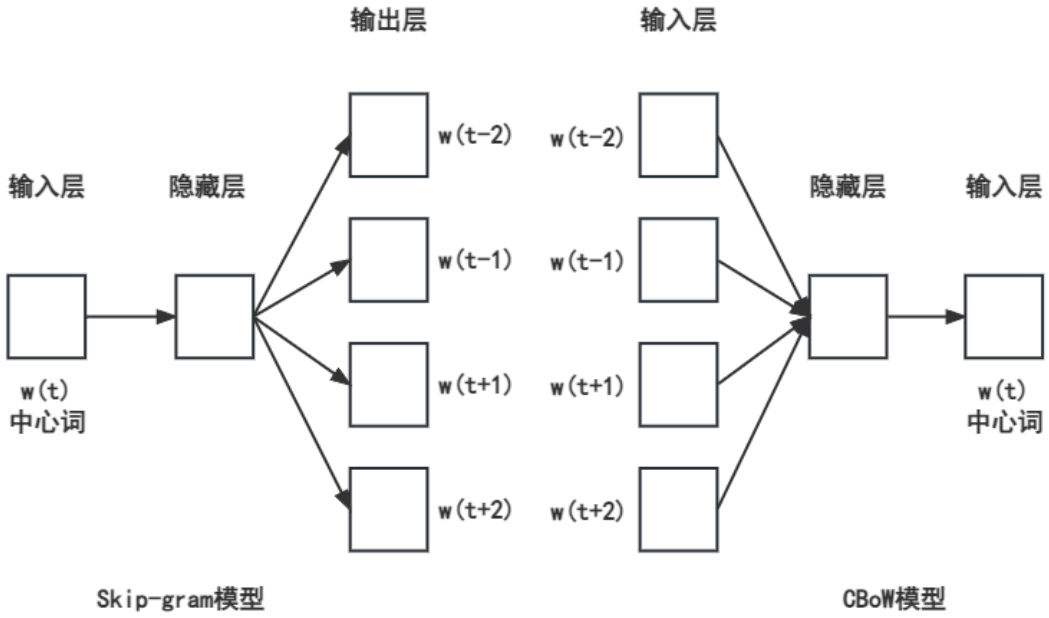


图2　Skip-gram和CBOW模型示意图

本文的文本数据为2006—2019年的A股上市公司年报数据，通过python获取上交所与深交所的官方网站相关年报文件，通过python将PDF格式的年报转换成TXT文本并进行文本数据清洗。年报通过jieba分词后，语料库规模约为12亿词频次，鉴于文本语料库的规模，本文模型的超参数设置为300维，感受窗口设置为20，最小词频设置为10。

得到训练后的词向量，将对所有种子词进行词向量余弦计算，对于给定的词语向量A和B，余弦相似度的计算方法为：

$$similarity = \cos(\theta) = \frac{\sum_{k=1}^{n} A_k * B_k}{\sqrt{\sum_{k=1}^{n}(A_k)^2}\sqrt{\sum_{k=1}^{n}(B_k)^2}} \quad (1)$$

余弦相似度越大，代表两个词语相关性越强。我们根据余弦相似度对每个种子词选取了相关性大于0.6的词语，作为“网络安全治理扩展词”的候选词。在候选词的基础上进行进一步筛选，筛选出了具有较强网络安全治理含义相关性的词语，作为网络安全治理的扩展词。

（四）词典展示

表2展示了我们构建的“网络攻击词典”的相关信息，分别展示了种子词和扩展词在全部年报

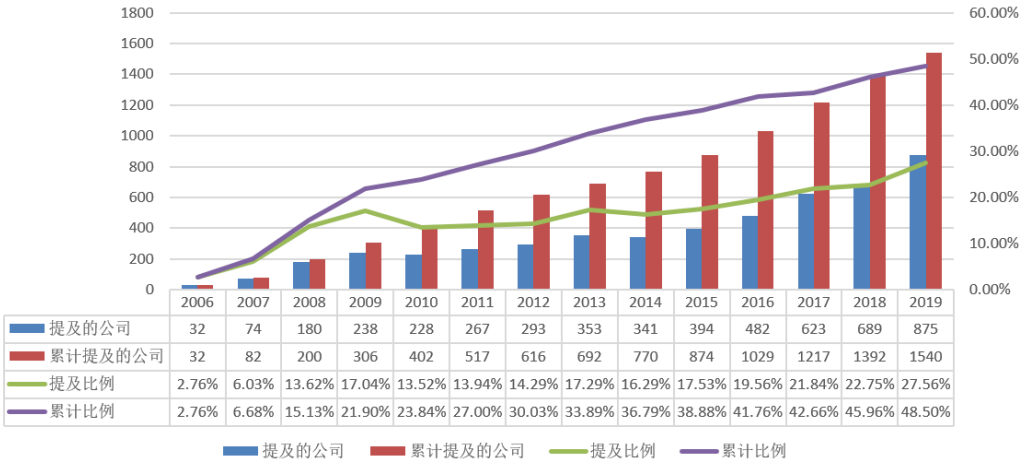
文本中出现的频次。我们发现网络安全扩展词有效补充了网络安全治理文本识别方法的感知范围，种子词典的词频为10599次，扩展词典的词频为45689次，原有的种子词典只占总频次的18.8%左右，种子词典涉及的上市公司数量为473家，种子词典与扩展词典涉及的上市公司数量为1540家。这突出了构建网络治理扩展词典的必要性。

表 2　　网络安全治理词典

种子关键词	频次	扩展关键词	频次	扩展关键词	频次	扩展关键词	频次
网络安全	7605	黑客攻击	110	安全漏洞	158	互联网安全	576
网络攻击	222	高危漏洞	18	入侵	871	容灾	461
数据泄露	110	蠕虫	15	恶意代码	31	灾备	1167
系统漏洞	36	恶意软件	48	宕机	20	网信	10614
计算机病毒	126	木马	111	崩溃	77	网安	3480
数据安全	2230	恶意程序	60	后门	140	系统安全	2397
拒绝服务	74	攻击者	38	劫持	27	敏感数据	78
访问控制	196	攻击行为	45	信息安全	22054	安全策略	130
		沙箱	30	数据备份	193	硬件安全	18
		数据库安全	38	加密技术	114	数据安全	2231
		篡改	302	加密传输	37		

（五）网络安全治理词典与治理情况概述

图3反映了2006—2019年间，4个不同层次网络安全治理情况的变化趋势。在2008年之前，鲜有公司披露网络安全治理情况；2008—2015年间，关注网络安全治理的公司数量平稳上升；2016年以后，关注网络安全治理的公司数量显著上升，这可能与2016年颁布的《中华人民共和国网络安全法》密切相关。截至2019年，有超过1/4的公司在当年年报中涉及了网络安全治理相关内容，累计有48.5%的公司在历史年报中涉及过网络安全治理事项，这与中央近年来越来越重视网络安全治理的趋势相吻合。



	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
提及的公司	32	74	180	238	228	267	293	353	341	394	482	623	689	875
累计提及的公司	32	82	200	306	402	517	616	692	770	874	1029	1217	1392	1540
提及比例	2.76%	6.03%	13.62%	17.04%	13.52%	13.94%	14.29%	17.29%	16.29%	17.53%	19.56%	21.84%	22.75%	27.56%
累计比例	2.76%	6.68%	15.13%	21.90%	23.84%	27.00%	30.03%	33.89%	36.79%	38.88%	41.76%	42.66%	45.96%	48.50%

图3 上市公司网络安全治理的情况

四、实证模型及数据

（一）样本选取与数据来源

为了考察网络安全治理对企业股价崩盘风险的影响，本文以2006—2019年中国A股市场上市公司作为研究对象，并依次剔除如下样本：（1）ST、*ST 和 PT 公司；（2）IPO当年的观测值和已退市的公司;（3）主要变量缺失的公司;（4）年度周收益率少于26个观测值的公司（Kim et al.，2011；权小锋等，2015）;（5）金融业的上市公司；（6）信息传输、软件和信息技术服务业的上市公司。网络安全领域属于信息传输、软件和信息技术服务业范畴，存在部分公司从事网络安全相关业务的情况，故本文将信息传输、软件和信息技术服务业数据剔除后进行后续分析。最终，获得共3174家上市公司26838个样本。上市公司财务数据主要来源于CSMAR，WIND等数据库。为了避免极端值的干扰，本文对连续变量进行上下1%的缩尾处理。

（二）变量定义

1. 股价崩盘风险

参考现有研究（Jin and Myers，2006；Kim et al.，2011；权小锋等，2015；彭俞超等，2018），本文主要采用两个基于周股票收益率的指标$Ncskew$、$Duvol$来衡量股价崩盘风险，具体计算过程如下。

首先，我们对每个年度的个股 i 的周收益率进行以下回归：

$$r_{i,t} = \beta_0 + \beta_1 r_{m,t-2} + \beta_2 r_{m,t-1} + \beta_3 r_{m,t} + \beta_4 r_{m,t+1} + \beta_5 r_{m,t+2} + \varepsilon_{i,t} \quad (2)$$

其中，$r_{i,t}$为股票i在某一年度第t周的收益率，$r_{m,t}$为市场在某一年度第t周的流通市值加权平均市场收益率，为调整非同步性交易的影响，模型（2）中加入了市场周收益的滞后项和超前项。取

上述回归的残差项，股票 i 在第 t 周的特有收益为：$W_{i,t}=\ln\left(1+\varepsilon_{i,t}\right)$。基于特有收益$W_{i,t}$，我们构建$Ncskew$、$Duvol$两个衡量股价崩盘风险的指标。

$Ncskew$为股票的负收益偏态系数，其数值越大，表示股票的崩盘风险越大，计算方法为：

$$Ncskew_{i,t}=-\frac{n(n-1)^{\frac{3}{2}}\sum w_{i,t}^{3}}{(n-1)(n-2)\left(\sum w_{i,t}^{2}\right)^{\frac{3}{2}}} \tag{3}$$

其中，n为股票i在当年交易的周数。第二个指标$Duvol$，为股票上下波动率的比例，计算方法为：

$$Duvol_{i,t}=\ln\left[\frac{n_u-1}{n_d-1}\frac{\sum_{Down}\ w_{i,t}^{2}}{\sum_{U_p}\ w_{i,t}^{2}}\right] \tag{4}$$

其中，n_u、n_d分别表示一年中股票周特有收益率大于、小于年平均收益率的周数。$Duvol$数值越大，表示股价崩盘风险越高。

2. 网络安全治理

本文将选取上市公司网络安全治理的指标定义为$Dcyber$，$Dcyber$为虚拟变量，即当公司年报中出现网络安全治理词典中的关键词次数大于1时为“1”，否则为“0”。大于1表示某上市公司在某年内至少一次对公司网络安全治理情况信息进行披露。这种衡量方式的基本假设是：上市公司披露的年报是基于公司实际运营情况客观的陈述，年报中网络安全治理相关关键词的出现与否能够较好地反映公司是否关注网络安全治理。在后文中，我们还引入其他指标进行稳健性检验。

3. 其他控制变量

根据已有研究（Kim et al.，2011；权小锋等，2015；彭俞超等，2018），我们控制了如下控制变量：企业规模$lnAssets$、公司权益乘数lev、公司年龄Ln_Age、固定资产比率PPE_TA、总资产收益率ROA、股票波动率$Sigma$、股票回报率Ret、市值账面比MB，具体参见表3。

表3　　主要变量定义与描述性统计

变量符号	变量定义	均值	标准差	中位数	观测数
$Ncskew$	向后一年股票周收益的负偏度，算法见公式(5)	-0.293	0.707	-0.261	26838
$Duvol$	向后一年股票周收益上下波动比率，算法见公式(6)	-0.198	0.482	-0.203	26838
$Dcyber$	上市公司是否关注网络安全治理	0.216	0.411	0	26838
$lnAssets$	总资产取自然对数	22.046	1.324	21.864	26838

lev	总资产除以股东权益	2.252	1.628	1.781	26838
Ln_Age	当年年份减去上市年份加1，再取自然对数	2.032	0.902	2.303	26838
PPE_TA	固定资产除以总资产	0.236	0.169	0.202	26838
ROA	净利润除以总资产	0.039	0.059	0.037	26838
$Sigma$	股票波动率，周股票特有收益的年标准差	0.048	0.018	0.045	26838
Ret	股票回报率，周股票特有收益的年平均值	-0.001	0.001	0.001	26838
MB	市值账面比，期末流通市值与期末股东权益账面价值之比	2.103	6.774	1.567	26838

（三）模型设定

为了研究网络安全治理对股价崩盘风险的影响，本文估计如下的回归模型:

$$Crashrisk_{i,j,t+1} = \alpha_0 + \alpha_1 Dcyber_{i,j,t} + \alpha_2 Controls_{i,j,t} + \gamma_j + \delta_t + \epsilon_{ijt} \quad (5)$$

其中，i代表企业，t代表年份，j代表行业；被解释变量$Crashrisk_{i,j,t+1}$是j行业的企业i在第$t+1$年的股价崩盘风险，由$Ncskew_{i,j,t+1}$与$Duvol_{i,j,t+1}$2个变量衡量；解释变量为$Dcyber_{i,j,t}$。模型中还控制了时间固定效应δ_t和行业固定效应γ_j，并对回归系数的标准误在企业层面进行了聚类处理。

五、实证结果与分析

（一）基准模型

首先，本文对上市公司是否披露网络安全治理情况与股价崩盘风险的关系进行验证。回归结果如表4所示。在第(1)~(2)列中，为了检验网络安全治理的直接影响，回归仅控制了年度—行业固定效应，未添加其他控制变量。可以看出，$Dcyber$的回归系数在两列中均在5%的统计水平上显著为负，这表明：关注网络安全治理的公司，其股价崩盘风险越低。为了进一步确认这一负向关系是否稳健成立，在第(3)~(4)列中，本文在回归中加入了一系列研究股价崩盘风险问题的控制变量，在此情况下，$Dcyber$的回归系数在1%的统计水平上显著为负。从经济意义上来看，关注网络安全治理情况的公司，可以使下一期的负收益偏态系数$Ncskew$与下一期的收益上下波动比率$Duvol$显著下降。这一经济影响与一些企业重要的财务指标影响是相当的，如企业资产规模与企业年限等。由此可见，无论从统计意义上还是从经济意义上，企业网络安全治理与未来的股价崩盘风险有着显著的负向关

系。

表4　　网络安全治理与股价崩盘风险

	(1)	(2)	(3)	(4)
	$F.Ncskew$	$F.Duvol$	$F.Ncskew$	$F.Duvol$
$Dcyber$	-0.029**	-0.029***	-0.026***	-0.029***
	(0.012)	(0.008)	(0.012)	(0.008)
$lnAssets$			-0.020***	-0.021***
			(0.005)	(0.003)
lev			0.016***	0.013***
			(0.004)	(0.002)
Ln_Age			-0.028***	-0.018***
			(0.008)	(0.005)
PPE_TA			-0.063*	-0.030
			(0.034)	(0.023)
ROA			-0.040	-0.115*
			(0.091)	(0.061)
$Sigma$			-0.856	-1.840**
			(1.249)	(0.841)
Ret			0.597***	0.310**
			(0.209)	(0.149)
MB			0.007***	0.004***
			(0.002)	(0.001)
Year /Industry FE	Yes	Yes	Yes	Yes
N	26838	26838	26838	26838
adj. R^2	0.058	0.063	0.085	0.092

（二）企业特征异质性影响

不同类型的公司对于网络安全重视程度有所不同，对于网络安全的投入成本也存在差异，管理层对网络安全治理的意识也不相同，这导致其网络安全治理对于股价崩盘风险的影响程度存在异质性。本文从产权性质、公司规模方面探究网络安全治理与股价崩盘风险的异质性。表5的结果表明国有企业相对于民营企业而言，网络安全风险治理对股价崩盘风险的影响更显著，资产规模较小的公司网络安全治理对股价崩盘风险的影响更显著。

表5　　网络安全治理与股价崩盘风险:异质性分析

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	F.Ncskew	*F.Ncskew*	*F.Duvol*	*F.Duvol*	*F.Ncskew*	*F.Ncskew*	*F.Duvol*	*F.Duvol*
样本	国有企业	民营企业	国有企业	民营企业	公司资产规模大	公司资产规模小	公司资产规模大	公司资产规模小
Dcyber	-0.049*** (0.015)	0.002 (0.015)	-0.034*** (0.011)	-0.005 (0.010)	-0.007 (0.014)	-0.038** (0.016)	-0.007 (0.010)	-0.031*** (0.011)
Controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year/Industry FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
difference	0.051		0.029		0.031		0.024	
p-value	0.006		0.032		0.021		0.034	
N	12107	14730	12107	14730	13446	13392	13446	13392
adj. R^2	0.099	0.064	0.103	0.071	0.093	0.073	0.094	0.082

（三）稳健性检验

本文的实证方法是用当期的网络安全治理情况与下一期的股价崩盘风险关系进行研究，这在一定程度上可以缓解由于反向因果带来的内生性问题。但是，股价崩盘风险高的上市公司，有可能出于获取正向收益的动机，主动披露网络安全治理信息从而带来正向反馈；另一方面，企业内部治理偏好与治理水平（如经理人背景等因素）会影响企业网络安全治理的决策，同时这些特征也会影响上市公司股价崩盘风险，这就会产生遗漏变量的问题。为了处理潜在的内生性问题，本文将从如下2个方面对企业网络安全治理与估计崩盘风险的关系进行检验，包括更换解释变量、加入其他控制变量。

1. 更换解释变量

鉴于年报文本表述的复杂性，本文使用“网络安全治理”关键词频密度描述上市公司对于网络安全治理的关注程度，具体而言，将上市公司“网络安全治理”关键词在年报中出现的总次数除以该年报的总词汇量，得到词频密度$density_{i,t}$。为了消除随时间增长的网络安全关注度影响，本文计算不同公司相同年份的词频密度的均值，记作Avr_t。我们设计一种虚拟变量$DcyberAvr_{i,t}$作为新的解释变量，将$density_{i,t}$>Avr_t的$DcyberAvr_{i,t}$设置为“1”，否则为“0”。这样做的经济学解释是：

$DcyberAvr_{i,t}$取值为“1”的上市公司管理层相对于所有A股上市公司管理层而言，透露了更多关于网络安全治理的相关信息，并且消除了随时间增长的网络安全关注度的影响。表6 Panel A报告了回归结果，可以发现，本文的主要结果在各列中仍显著成立。

此外，我们更换解释变量为公司年报中披露网络安全治理相关关键词的频次+1后取对数$lncyber$，回归结果如表6 Panel B所示。可以看出，$lncyber$的回归系数仍然显著为负。从经济意义上来看，以(3)~(4)为例，披露一个“网络安全治理”相关关键词的公司的下一期负收益偏态系数$Ncskew$，比没有披露任何相关关键词的公司平均而言降低4% ($\ln 2 * -0.017/-0.293$)，而下一期的收益上下波动比率$Duvol$平均而言降低4.2% ($\ln 2 * -0.012/-0.198$)。

这一部分表示，本文所发现的网络安全治理对股价崩盘风险的影响是稳健的。

表6　　更换解释变量

Panel A:更换均值解释变量$DcyberAvr$				
	(1)	(2)	(3)	(4)
	$F.Ncskew$	$F.Duvol$	$F.Ncskew$	$F.Duvol$
$DcyberAvr$	-0.019*	-0.015**	-0.024**	-0.020***
	(0.011)	(0.007)	(0.011)	(0.007)
Controls	No	No	Yes	Yes
Year /Industry FE	Yes	Yes	Yes	Yes
N	26838	26838	26838	26838
adj. R^2	0.052	0.057	0.077	0.083
Panel B:更换对数解释变量$lncyber$				
	(1)	(2)	(3)	(4)
	$F.Ncskew$	$F.Duvol$	$F.Ncskew$	$F.Duvol$
$lncyber$	-0.021**	-0.013**	-0.017*	-0.012**
	(0.009)	(0.006)	(0.009)	(0.006)
Controls	No	No	Yes	Yes
Year /Industry FE	Yes	Yes	Yes	Yes
N	26838	26838	26838	26838
adj. R^2	0.049	0.053	0.074	0.079

2. 加入其他控制变量

因为可能存在难以观测的因素同时与公司网络安全治理水平和股价崩盘风险相关。正如前文提到的管理层股权结构与产权性质所导致的企业决策管理差异，同时影响了公司网络安全治理水平和股价崩盘风险。因此，本文通过在回归模型中加入其他公司治理层面的控制变量，缓解因遗漏变量因素带来的内生性，如表7所示。

在第(1)～(2)列，加入了第一大股东持股占总股数的比重$Sh1$；在第(3)～(4)列，加入了董事会规模$Board_Size$；在第(5) ～(6)列，加入了股权国有性质SOE；在第(7) ～(8)列，控制了上述全部的控制变量。可以看出，本文的主要发现在各列中显著成立。

表7　　加入其他控制变量

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	$F.Ncskew$	$F.Duvol$	$F.Ncskew$	$F.Duvol$	$F.Ncskew$	$F.Duvol$	$F.Ncskew$	$F.Duvol$
$Dcyber$	-0.014**	-0.017***	-0.014**	-0.017***	-0.014**	-0.017***	-0.014**	-0.017***
	(0.011)	(0.007)	(0.011)	(0.007)	(0.011)	(0.007)	(0.011)	(0.007)
$Sh1$	-0.004	0.003					-0.001	0.005
	(0.030)	(0.021)					(0.031)	(0.021)
SOE			-0.018**	-0.009			-0.019**	-0.010
			(0.010)	(0.007)			(0.011)	(0.007)
$Board\_Size$					0.003	0.001	0.005	0.003
					(0.023)	(0.016)	(0.023)	(0.016)
Controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year/Industry FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
N	26838	26838	26838	26838	26837	26837	26837	26837
adj. R^2	0.077	0.083	0.077	0.083	0.077	0.083	0.077	0.083

注：本报告中系数为标准化β系数。

六、进一步讨论

（一）机制分析

1. 网络安全治理与企业信息不对称的影响

现有文献对于个股股价崩盘风险的研究主要基于Jin and Myers（2006）的坏消息隐藏假说，该假说认为股价崩盘风险主要由于上市公司所隐藏的负面消息突然暴露所导致，对治理信息披露可以降低企业与投资者之间的信息不对称，从而降低股价崩盘风险（叶康涛等，2015）。

通过对公司网络安全治理信息披露是否直接影响企业与外界的信息不对称程度进行检验，我们发现公司的网络安全治理信息披露降低了公司与外界投资者的信息不对称，从而缓解了股价崩盘风险。参考彭俞超等（2018）的研究中关于企业信息不对称的测度方法，选取了会计稳健性指标$Cscore$和$Gscore$与KV指数作为被解释变量，其中$Cscore$指标越高，说明企业盈余对坏消息的灵敏度越高，企业的会计稳健性越强；$Gscore$指标越高，说明企业会计盈余对好消息的灵敏度越高；KV指数越低，意味着企业信息披露的程度越高。回归结果如表8所示，结果表明：网络安全治理的披露对应着$Cscore$的上升、$Gscore$和KV的下降，这说明网络安全治理信息披露使得企业对坏消息的披露更加及时，而不会盲目披露好消息，从而降低了股价崩盘风险。

表8　　网络安全治理与信息不对称

	(1)	(2)	(3)
	$Cscore$	$Gcsore$	KV
$Dcyber$	0.028**	-0.020**	-0.020***
	(0.014)	(0.010)	(0.003)
Controls	Yes	Yes	Yes
Year/Industry FE	Yes	Yes	Yes
N	22475	22475	22475
adj. R^2	0.116	0.151	0.116

2. 网络安全治理对企业社会责任的影响

已有研究表明，一个社会责任较高的企业，会增加投资者对于公司的信心，从而降低股价崩盘风险（黄金波等，2022）。企业网络安全主体责任是企业社会责任的重要组成部分，企业加强网络安全治理，有助于企业提高自身的社会责任，增加投资者对于企业的信心，从而降低股价崩盘风险。本文选用和讯网统计的企业社会责任指数CSR探究网络安全治理对企业社会责任的影响，该企业社会责任评分数据覆盖2010—2019年，从股东责任、员工责任、供应商和消费者权益责任、环境责任与社会责任5个方面分别设定标准进行评分，得分越高，说明企业社会责任履行得越好。剔除缺失样本后，以网络安全治理相关的企业社会治理总评分的对数$lnCSR$、员工责任评分的对数$lnCSR_1$、社会责任评分的对数$lnCSR_2$等为被解释变量，回归模型验证网络安全治理对企业社会责任的影响，结果如表9。回归结果表明，网络安全治理显著提高了总评分、员工社会责任评分和社会责任评分。

表9　　网络安全治理与企业社会责任

	(1)	(2)	(3)
	$lnCSR$	$lnCSR_1$	$lnCSR_2$
$Dcyber$	0.021**	0.061***	0.034***
	(0.009)	(0.018)	(0.014)
Controls	Yes	Yes	Yes
Year/Industry FE	Yes	Yes	Yes
N	19686	19686	19686
adj. R^2	0.384	0.220	0.309

（二）《网络安全法》出台的准自然实验分析

为进一步验证网络安全治理与股价崩盘风险是否存在反向因果关系，本文使用2016年颁布的《中华人民共和国网络安全法》作为外生冲击，构建双重差分（DID）模型进行准自然实验检验。根据以往的研究，外部监管要求变化会影响企业网络安全治理结构及相关信息披露的策略。比如，美国SOX法案促进了企业的网络安全信息披露（Gordon et al.，2006）；泄露信息披露法促进了企业加强网络安全管理，则企业数据泄露事件会减少（Ashraf and Sunder，2020）。网络安全法是国家为保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展而制定的法律。网络安全法对网络安全、监测预警、应急处置作出相关规定，也规定了各个主体网络安全责任与法律责任。因此，网络安全法的实施大大加强了企业网络安全治理。

由于网络安全法是普适性法律，难以通过一般方法确定处理组和控制组。因此，本文首先计算2015—2017年年报文本中网络安全治理关键词的数量变化，再将关键词数量逐年升高的企业设置为处理组，共计440家上市公司。这样的含义是：该上市公司受到《中华人民共和国网络安全法》的影响，加强了网络安全治理，因此被设置为被处理组。在剩余的企业中，我们通过倾向评分匹配法(PSM)选取一组与处理组中在主要财务指标上相似的企业构建对照组来进行分析，对照组的筛选使用logit回归和一对一最近邻匹配法。logit回归的被解释变量为是否为关键词数量逐年升高的虚拟变量，解释变量为本文基准模型中的控制变量，并计算出每个样本的倾向得分。再对关键词数量没有逐年升高的样本进行一对一最近邻匹配，筛选出倾向得分最接近的样本，从而生成对照组样本，共计440家上市公司。

在确立了处理组与对照组之后，本文设置了如下2个关键变量：虚拟变量$Treat_i$表示i公司是否

为处理组，如果是处理组，$Treat_i$=1；如果是对照组，$Treat_i$=0。$Post_t$同样是一个虚拟变量，对于2016年及之后年度，$Post_t = 1$，对于2016之前的年度，$Post_t = 0$。本部分采用的实证检验模型如下：

$$Crashrisk_{i,t+1} = \alpha_0 + \alpha_1 Treat_i + \alpha_2 Post_t + \alpha_3 Treat_i * Post_t + \alpha_4 Controls_{it} + \epsilon_{it} \quad (6)$$

其中，解释变量$Crashrisk_{i,t+1}$与控制变量$Controls_{it}$的设置与我们的主要模型相同；$Treat_i$代表公司是否属于处理组；$Post_t$代表样本是否归属于2016年及之后区间。交互项系数α_3是我们感兴趣的部分，因为它刻画了《中华人民共和国网络安全法》的颁布对企业股价崩盘风险的净效应。

在进行回归以前，本文根据实践检验的方法对本模型的平行趋势假设进行了检验，检验结果如图4所示，结果表明在网络安全法颁布的2016年以前，交乘项系数均不显著，说明处理组与对照组的政策交乘项系数无显著差异。而网络安全法颁布后，处理组与对照组交乘项系数差异显著异于0，且连续2年降低，这说明网络安全法的实施对企业股价崩盘风险有着显著负向作用，且政策具有一定的持续性，效用也在上升。

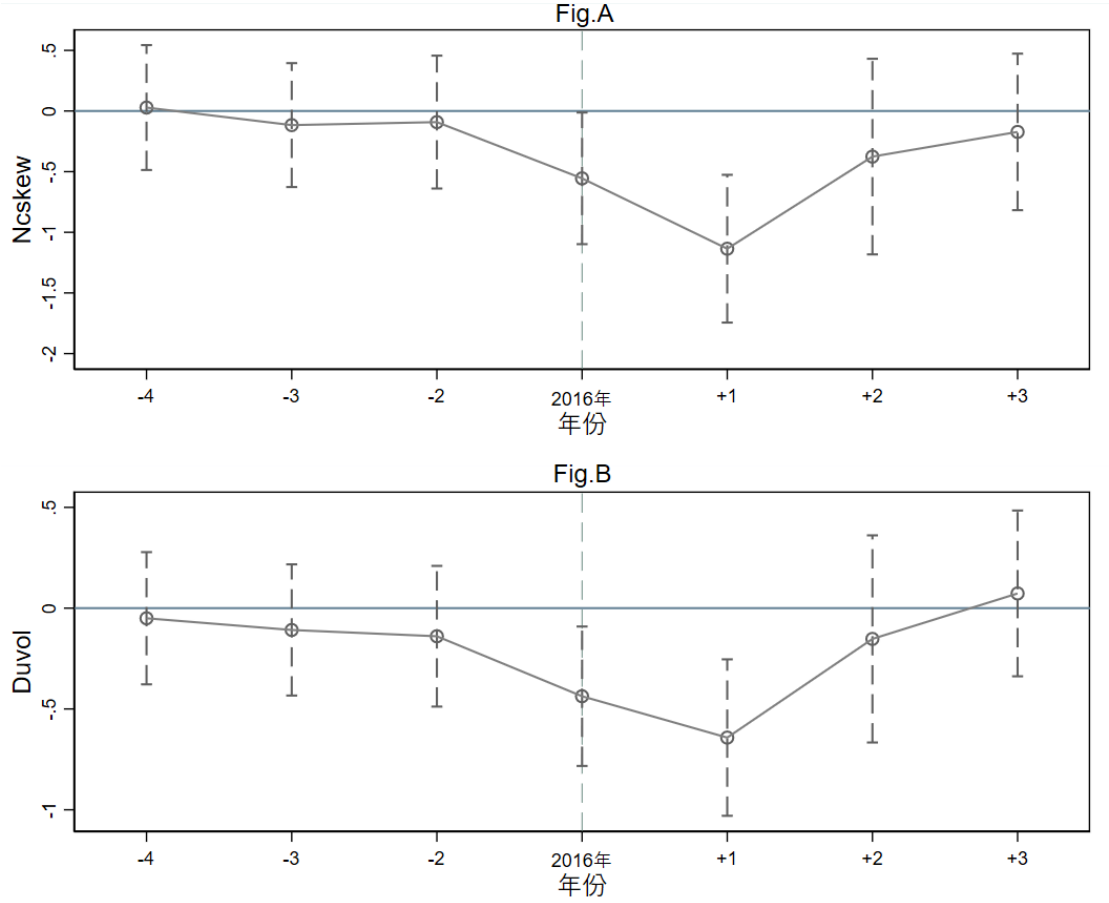


图4 平行趋势检验

表10报告了回归的结果，所有的回归结果均表明，网络安全法的实施，对企业股价崩盘风险具

有显著负向影响，并且都在1%水平下显著，从而缓解了因反向因果带来的内生性问题。

表10　　双重差分法检验

	(1)	(2)
	$F.Ncskew$	$F.Duvol$
$Treat*Post$	-0.318***	-0.215***
	(0.077)	(0.049)
$Treat$	0.167***	0.102***
	(0.054)	(0.035)
$Post$	0.323***	0.237***
	(0.071)	(0.046)
Controls	Yes	Yes
N	3941	3941
adj. R^2	0.022	0.026

（三）网络安全治理程度的影响因素分析

公司网络安全治理作为公司治理的重要部分，本小节将着重讨论影响企业关注网络安全治理的因素，本文参考了张叶青等（2021）的方法，采用Probit（公式2）和OLS模型（公式3）模型分析影响网络安全治理情况的因素：

$$Prob(Dcyber_{ijpt}=1)=\phi(\beta_0+\beta_1 X_{i,j,p,t-1}+Ind_j+year_t+pro_p) \quad (7)$$

$$lncyber_{ijpt}=\beta_0+\beta_1 X_{i,j,p,t-1}+Ind_j+year_t+pro_p \quad (8)$$

其中，i代表企业，t代表年份，p代表省份，j代表行业；公式（7）的被解释变量为公司年报中是否提及网络安全治理相关关键词的虚拟变量（$Dcyber_{ijpt}$）；公式（8）的被解释变量为公司年报中披露网络安全治理相关关键词的频次+1后取对数（$lncyber_{ijpt}$）。$X_{i,j,p,t-1}$代表一系列可能影响公司网络安全治理程度的滞后一期变量。其中，财务指标主要包括：公司规模$lnAssets_{i,j,p,t-1}$，杠杆率$Lev_{i,j,p,t-1}$，公司年龄$Ln_Age_{i,j,p,t-1}$，固定资产比率$PPE_TA_{i,j,p,t-1}$，总资产收益率$ROA_{i,j,p,t-1}$，销售收入增长率$SalesGrowth_{i,j,p,t-1}$，股权国有性质$SOE_{i,j,p,t-1}$，公司成长性指标$TobinQ_{i,j,p,t-1}$。企业治理变量包括：第一大股东持股比例$Sh1_{i,j,p,t-1}$，第一大股东持股占总股数的比重；董事会规模$Board_Size_{i,j,p,t-1}$，董事会人数取对数。模型中还控制了时间固定效应$year_t$、行业固定效应Ind_j与省份固定效应pro_p，并对回归系数的标准误在企业层面进行了聚类处理。

表11汇报了网络安全治理程度的决定性因素分析结果。第（1）列、第（2）列的被解释变量

为网络安全治理的虚拟变量（$Dcyber$）并采用Probit模型进行估计。第（1）列控制了时间和行业层面的固定效应，第（2）列额外控制了省份层面的固定效应。第（3）列、第（4）列报告了基于网络安全治理程度的连续变量（$lncyber$）的分析，第（3）列同样控制了时间和行业层面的固定效应，第（4）列额外控制了省份层面的固定效应。综合表3的结果，我们发现：一是规模越大、成长性越好的公司越重视网络安全治理。这可能是因为规模越大、成长性越好的公司更加重视自身的企业风险与潜在声誉，所以更加重视网络安全风险，同时规模越大、成长性越好的公司也拥有充足的资金进行网络安全的治理。二是相对于民营企业来说，国有企业更关注网络安全治理。这可能是因为国有企业更加重视企业的社会责任，同时国有企业的网络安全治理也受到上级监管部门的监督。三是固定资产比例越低的企业越重视网络安全治理。这可能是因为固定资产比例越低的企业数字化程度越高（张叶青等，2021），数字化程度越高的企业对网络安全治理的需求越大。四是股权相对分散的上市公司更重视网络安全治理。这可能是因为股权相对分散的上市公司风险承担意识更强（Dhillon and Rossetto，2015），这可能导致公司决策对网络安全风险更加厌恶，从而更加关注网络安全治理。

表11　　网络安全治理情况的影响因素

	(1)	(2)	(3)	(4)
	$Dcyber$	$Dcyber$	$lncyber$	$lncyber$
$L.lnAssets$	0.125***	0.118***	0.048***	0.046***
	(0.011)	(0.011)	(0.008)	(0.008)
$L.Lev$	-0.021**	-0.020**	-0.004	-0.004
	(0.008)	(0.008)	(0.004)	(0.004)
$L.ln\_Age$	-0.068***	-0.065***	-0.016*	-0.014
	(0.016)	(0.016)	(0.009)	(0.009)
$L.PPE\_TA$	-0.381***	-0.353***	-0.239***	-0.229***
	(0.079)	(0.080)	(0.051)	(0.050)
$L.ROA$	-0.075	0.009	-0.033	-0.002
	(0.213)	(0.214)	(0.112)	(0.113)
$L.SalesGrowth$	0.003	0.001	-0.007	-0.008
	(0.021)	(0.021)	(0.006)	(0.006)
$L.SOE$	0.084***	0.051*	0.041**	0.034*
	(0.026)	(0.027)	(0.019)	(0.019)
$L.TobinQ$	0.044***	0.038***	0.013***	0.011**
	(0.010)	(0.011)	(0.005)	(0.005)

L.Sh1	-0.003*** (0.001)	-0.002*** (0.001)	-0.001** (0.001)	-0.001** (0.001)
L.Board_Size	-0.064 (0.055)	-0.052 (0.055)	-0.018 (0.037)	-0.015 (0.037)
固定效应	Year, Industry	Year, Industry, Province	Year, Industry	Year, Industry, Province
N	26883	26883	25516	25516
pseudo R^2	0.113	0.118		
adj. R^2			0.119	0.123

注: *、**、***分别表示在10%、5%、1%的水平上显著。以下同。

七、结论

本文利用中国A股上市公司披露的年报，使用基于深度学习的Word2vec自然语言处理技术，构造并扩展了网络安全治理关键词，利用非结构化的文本数据构造了中文语境下的上市公司网络安全治理的度量指标，并基于此展现了中国上市公司网络安全治理的现实情况，分析了公司网络安全治理的影响因素。相对于过往研究，使用深度学习模型与自然语言处理技术有效增强了对于网络攻击治理此类小样本事件的获取能力，并能更好的刻画中国上市公司网络安全治理情况的变化，为后续研究提供了可靠的数据基础。

更重要的是，本文研究了网络安全治理对企业股价崩盘风险的影响及其作用机制，为网络安全治理和金融市场稳定提供了实证依据。本文发现，网络安全治理可以显著降低股价崩盘风险，提高金融市场稳定。具体机制分析表明，一方面，企业网络安全治理使得企业对不利消息的披露更加及时，而不会盲目披露好消息，从而降低了股价崩盘风险；另一方面，网络安全治理也可以提高企业社会责任，增加投资者对于公司的信心，从而降低股价崩盘风险。本文采用《中华人民共和国网络安全法》作为外生冲击构建了双重差分检验的方法，缓解了内生性问题，得到了一致结论。异质性分析表明，不同公司在公司治理层面对网络安全治理的重视程度不同：国有企业、规模较大、公司成长性较好、有形资产比例较低的公司，重视网络安全治理的可能性更高。另外，网络安全治理对于股价崩盘风险的降低在市值规模小的企业和国有企业中更为显著。

基于上述研究结论，我们对于中国网络安全治理与金融风险防范的政策提出下几点建议：

第一，企业自身应注重提高内部控制管理质量，通过聘任技术背景高管、加大网络安全设备人才投入等方式，加强网络安全治理，维护企业的核心价值。在数字经济快速发展与企业高度信息化转型的时代背景下，企业加强网络安全治理，对于保证自身生产经营安全、维护自身信誉，乃至

于维护金融市场稳定尤为关键。

第二，在国际局势错综复杂，贸易保护主义、民粹主义势头升级，网络攻击全球化、常态化的背景下，各类社会主体都应更加重视网络安全治理。网络安全事件会造成企业股价崩盘、声誉受损、核心数据资产丢失以及法律成本增加等多方面负面影响，有可能会影响企业长期价值。投资者、分析师、审计师、债权人、政府监管部门等多主体应该更加全面地了解企业网络安全风险与治理情况对公司财务、资产价格、经营状况的影响，更加精准地考察企业风险与风险治理情况，以便作出更加科学合理的决策。

第三，政府监管部门应履行好网络安全治理的监管责任。鉴于网络安全事件的严重后果，目前中国金融市场监管部门对于上市公司网络安全治理的监管仍不够到位，仅在《企业内部控制应用指引第18号——信息系统》提及“企业应采用防火墙等手段加强网络安全”。相比之下，美国证券交易委员会前后两次发布《网络安全风险披露报告指南》，强制要求在美股上市的规模以上上市公司必须及时向投资者汇报可能影响公司经营的网络安全风险和治理情况。对于金融市场而言，风险信息披露可以大幅降低投资者与上市公司之间的信息不对称，从而降低股价崩盘风险，促进金融市场稳定发展。因此，金融监管部门应联合网络安全归口部门应对于中国上市公司提出有关网络安全治理的信息披露要求。

参考文献

（1）Ashraf, M. and Sunder, J., 2020, "Does consumer protection regulation benefit shareholders? Evidence from data breach disclosure laws and the cost of equity", Working paper, Michigan State University and University of Arizona ….

（2）Callen, J. L. and Fang, X., 2013, "Institutional investor stability and crash risk: Monitoring versus short-termism?", *Journal of Banking & Finance*, 37(8), pp. 3047~3063.

（3）Coval, J. D. and Moskowitz, T. J., 1999, "Home bias at home: Local equity preference in domestic portfolios", *The Journal of Finance*, 54(6), pp. 2045~2073.

（4）Deng, S., Mao, C. X. and Xia, C., 2021, "Bank geographic diversification and corporate innovation: evidence from the lending channel", *Journal of Financial and Quantitative Analysis*, 56(3), pp. 1065~1096.

（5）Dhillon, A. and Rossetto, S., 2015, "Ownership structure, voting, and risk", *The Review of Financial Studies*, 28(2), pp. 521~560.

（6）Eisenbach, T. M., Kovner, A. and Lee, M. J., 2022, "Cyber risk and the US financial system: A pre-mortem analysis", *Journal of Financial Economics*, 145(3), pp. 802~826.

（7）Feng, C. Q. and Wang, T., 2019, "Does CIO risk appetite matter? Evidence from information security breach incidents", *International Journal of Accounting Information Systems*, 32, pp. 59~75.

（8）Gordon, L. A., Loeb, M. P., Lucyshyn, W. and Sohail, T., 2006, "The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities", *Journal of Accounting and Public Policy*, 25(5), pp. 503~530.

（9）Graham, J. R., Harvey, C. R. and Rajgopal, S., 2005, "The economic implications of corporate financial reporting", *Journal of accounting and economics*, 40(1-3), pp. 3~73.

（10）Hutton, A. P., Marcus, A. J. and Tehranian, H., 2009, "Opaque financial reports, R2, and crash risk", *Journal of Financial Economics*, 94(1), pp. 67~86.

（11）Jin, L. and Myers, S. C., 2006, "R2 around the world: New theory and new tests", *Journal of Financial Economics*, 79(2), pp. 257~292.

（12）Kamiya, S., Kang, J., Kim, J., Milidonis, A. and Stulz, R. M., 2021, "Risk management, firm reputation, and the impact of successful cyberattacks on target firms", *Journal of Financial Economics*, 139(3), pp. 719~749.

（13）Kim, J., Li, Y. and Zhang, L., 2011, "Corporate tax avoidance and stock price crash risk: Firm-level analysis", *Journal of Financial Economics*, 100(3), pp. 639~662.

（14）Kothari, S. P., Shu, S. and Wysocki, P. D., 2009, "Do managers withhold bad news?", *Journal of Accounting Research*, 47(1), pp. 241~276.

（15）Kwon, J., Ulmer, J. R. and Wang, T., 2013, "The association between top management involvement and compensation and information security breaches", *Journal of Information Systems*, 27(1), pp. 219~236.

（16）Li, K., Mai, F., Shen, R. and Yan, X., 2021, "Measuring corporate culture using machine learning", *The Review of Financial Studies*, 34(7), pp. 3265~3315.

（17）Li, X., Wang, S. S. and Wang, X., 2017, "Trust and stock price crash risk: Evidence from China", *Journal of Banking & Finance*, 76, pp. 74~91.

（18）Mikolov, T., Chen, K., Corrado, G. and Dean, J., 2013, "Efficient estimation of word representations in vector space", *arXiv preprint arXiv:1301.3781*

（19）Nordlund, J., 2021, "The Disclosure of Cybersecurity Risk", *Available at SSRN 3077632*

（20）Piotroski, J. D., Wong, T. J. and Zhang, T., 2015, "Political incentives to suppress negative information: Evidence from Chinese listed firms", *Journal of Accounting Research*, 53(2), pp. 405~459.

（21）Steinbart, P. J., Raschke, R. L., Gal, G. and Dilla, W. N., 2013, "Information security professionals' perceptions about the relationship between the information security and internal audit functions", *Journal of Information Systems*, 27(2), pp. 65~86.

（22）Vincent, N. E., Higgs, J. L. and Pinsker, R. E., 2017, "IT governance and the maturity of IT risk management practices", *Journal of Information Systems*, 31(1), pp. 59~77.

（23）卞世博、陈曜、汪训孝：《高质量的互动可以提高股票市场定价效率吗?——基于“上证e互动”的研究》，《经济学(季刊)》，2022年第03期。

（24）黄金波、陈伶茜、丁杰：《企业社会责任、媒体报道与股价崩盘风险》，《中国管理科学》，2022年第03期。

（25）江轩宇、许年行：《企业过度投资与股价崩盘风险》，《金融研究》，2015年第08期。

（26）李文贵、路军：《网络平台互动与股价崩盘风险:“沟通易”还是“操纵易”》，《中国工业经济》，2022年第07期。

（27）林润辉、谢宗晓、王兴起、魏军：《制度压力、信息安全合法化与组织绩效——基于中国企业的实证研究》，《管理世界》，2016年第02期。

（28）彭俞超、倪骁然、沈吉：《企业“脱实向虚”与金融市场稳定——基于股价崩盘风险的视角》，《经济研究》，2018年第10期。

（29）权小锋、吴世农、尹洪英：《企业社会责任与股价崩盘风险:“价值利器”或“自利工具”?》，《经济研究》，2015年第11期。

（30）尚兆燕、刘凯扬：《IT 控制缺陷, 财务报表重大错报风险及非标审计意见——来自中国上市公司的经验数据》，《审计研究》，2019年第1期。

（31）王秦、朱建明：《信息安全事件对公司价值的影响》，《技术经济》，2018年第2期。
（32）谢德仁、郑登津、崔宸瑜：《控股股东股权质押是潜在的“地雷”吗?——基于股价崩盘风险视角的研究》，《管理世界》，2016年第05期。
（33）叶康涛、曹丰、王化成：《内部控制信息披露能够降低股价崩盘风险吗?》，《金融研究》，2015年第02期。
（34）张叶青、陆瑶、李乐芸：《大数据应用对中国企业市场价值的影响——来自中国上市公司年报文本分析的证据》，《经济研究》，2021年第12期。
（35）赵静、黄敬昌、刘峰：《高铁开通与股价崩盘风险》，《管理世界》，2018年第01期。
（36）甄杰、谢宗晓、李康宏、林润辉：《信息安全治理与企业绩效：一个被调节的中介作用模型》，《南开管理评论》，2020年第01期。
（37）姜富伟、孟令超、唐国豪：《媒体文本情绪与股票回报预测》，《经济学(季刊)》，2021年第04期。