【信息披露】

《证券法苑》(2026)
第四十三卷,第 1~25 页

上市公司网络安全信息强制披露的逻辑基础与制度回应*

曹兴权** 张永森***

摘要:网络安全信息构成数据时代上市公司价值反映的增量,借由信息披露缓解因网络安全风险引发的代理问题已是世界范围内的治理共识。鉴于自愿披露在信息供给与外部性治理上的失灵,引入网络安全信息强制披露制度已属必要。通过对披露内容和适用范围做差异化安排能够在回应投资者保护的同时避免过度加重上市公司成本:披露内容应涵盖网络安全事件与网络安全风险治理三级信息,并设置披露例外情形;适用范围应区分不同行业、规模与板块的上市公司。

关键词:数据资产 网络安全 强制信息披露 重大性 差异化

---

* 本文系四川省哲学社会科学重点研究基地社会治理创新研究中心 2025 年一般项目"总体国家安全观视域下金融安全法治体系的完善路径研究"(批准号:SHZLYB2505)、四川警察学院智慧警务与国家安全风险治理重点实验室 2024 年度开放课题"统筹发展和安全视域下成渝经济圈金融安全的法治保障研究"(批准号:ZHKFQN2403)的阶段性成果。

** 西南政法大学民商法学院教授,法学博士。

*** 西南政法大学民商法学院博士研究生。

引　言

滴滴公司和中国知网因网络安全问题先后受到国家互联网信息办公室处罚的消息,引发了社会对上市公司网络安全风险的高度关注。上市公司发生网络安全事件带来了诸多严重后果,其网络安全治理受到了世界范围内监管者的关注,信息披露制度因其独特的制度优势,成为实现对上市公司网络安全监管的一个重要手段。

在我国,证券交易所已经通过若干自律指引探索性地将网络安全纳入了披露要求。例如,深交所最新的自律披露文件中要求从事网络安全相关业务的公司披露行业政策、资质信息和重大泄露事件;对从事电子商务业务、互联网营销及数据服务相关业务、快递等行业的公司,则在定期报告和风险提示中增设了数据安全、信息系统故障及泄露事件的披露要求。〔1〕这些规定具有一定针对性,但覆盖范围有限,且以鼓励性、指引性为主。与此同时,市场实践已显示出更为广泛的网络安全披露趋势。通过巨潮资讯网的检索,目前我国资本市场上披露网络安全的上市公司除指引中所列的行业外,互联网和相关服务行业、制造业、电力热力供应业、金属冶炼和压延加工业、金融业,甚至石油开采业的上市公司也通过年报、临时公告或 ESG 报告的方式主动披露网络安全信息。例如,电子设备制造业的海康威视在其定期报告中提示了网络安全风险,并披露了网络安全风险管理情况;制造业的中铁装配在定期报告中披露了公司的网络安全项目;化学制品制造业的鲁北化工通过 ESG 报告披露了其采取了的网络安全风险管理措施。然而,从披露的内容和质量来看,实践中存在明显差异。例如,就网络安全管理信息而言:吉比特在定期报告中详细披露了其网络安全风险管理团队人员构成、团队资质信息、数据流动各环节网络安全防控措施;而山石网科则仅以不到 200 字笼统

〔1〕参见《深圳证券交易所上市公司自律监管指引第 3 号——行业信息披露(2025 年修订)》《深圳证券交易所上市公司自律监管指引第 4 号——创业板行业信息披露(2023 年修订)》。

介绍其存在信息安全管理体系和管理流程。就网络安全事件信息而言：环旭电子详细披露了网络攻击源头、采取的措施、带来的影响、风险提示；而圣晖集成仅笼统披露了所采取的措施和事件影响（未造成影响）。

可见，我国资本市场中网络安全披露在披露范围上呈现出规则与实践的脱节，在披露内容上表现出缺乏统一标准，信息质量参差不齐。而随着数据资产“入表”的加速，网络安全水平已直接关联企业价值与投资者决策，仅依赖自律和自愿披露，将无法满足资本市场对透明度和投资者保护的要求。〔2〕由此，构建统一而审慎的网络安全强制披露制度，不仅是回应市场现实的必要之举，更是完善资本市场监管的一个重要课题。

特别需要说明的是：与网络安全有关的概念共有三个，分别是信息安全（Information Security）、狭义的网络安全（Network Security）与广义的网络安全（Cybersecurity）。信息安全指向上市公司所有信息的安全，不仅包括物理形态存在的信息，还包括电子化的信息；狭义的网络安全指向技术性的安全，如网络基础设施安全和通信安全。本文所讨论的是广义的网络安全，不仅涵盖了网络技术性安全和信息安全，更强调维持安全的状态，即保持个人，组织或者国家处于一种免受网络攻击的安全状态以及为此采取的措施，其中的重点是主动采取措施应对可能的网络安全风险。

一、上市公司披露网络安全的逻辑起点

（一）数据时代上市公司价值反映的增量

上市公司的管理层披露网络安全信息的首要原因是对融资的需要。为了吸引资本市场上有限的资本，上市公司的管理层会向市场传达出证明公司具有价值的信息。在数字时代，上市公司的价值突出表现为所拥有的数据资产，数据资产成为吸引投资者的重要因素。而数据资产的价值基础又在于数据安全，反映为上市公司的网络安全状况。由此，网络安全信息成为评价数据资产价值的关键信息，也是上市公司管理者可向

〔2〕 参见苑泽明、于翔、李萌：《数据资产信息披露、机构头投资者异质性与企业价值》，载《天津财经大学学报》2022年第11期。

市场传达出的特异信息。

1. 数据:上市公司资产的组成

从会计学的视角,资产是企业过去的交易或者事项形成的、由企业拥有或者控制的、预期会给企业带来经济利益的资源。这一概念给出了资产的两个特性,一是可控性,资产必须是企业能够控制的资源;二是经济性,资产必须是能给企业带来经济利益的资源。当前,数据已经被确立为继土地、劳动力、资本、技术等传统生产要素之后新的生产要素,数据资产已然是上市公司资产的重要组成部分。[3] 这一资产的形态表现为公司储存的客户信息、财务记录和知识产权等。从实际来看,数据作为一种资源在上市公司的生产经营中发挥了巨大的作用,其不仅能提高公司的销售业绩,例如,帮助企业精准定位用户群体,在促成交易方面发挥作用,还能帮助公司调整战略布局,公司可通过分析客户、合作伙伴、竞争对手的数据,提前对市场的发展做出预测,进而及时调整战略。因而,数据资产满足经济性和可控性的资产要求。数据之于公司如此重要,以至于出现了专门以数据抓取和挖掘为生的上市公司。统计显示,《企业数据资源相关会计处理暂行规定》于2024年1月1日正式实施后,上市公司披露数据资产的数量持续上涨,2024年一季度仅为17家,至2025年9月1日,共有110家上市公司披露了数据资产,涉及通信、计算机、软件、金融、制造等27个行业。[4] 披露数据资产的上市公司数量持续上涨,行业范围不断扩大,显示出数据资产已不再是隐性资源,而是投资者定价的重要参考。

2. 网络安全:数据资产价值的指标

有效市场假说所构建的证券信息与股票价格的分析框架为判断资本市场中哪些信息应予披露的"价格测试"提供了支撑。[5] 价格测试的核心在于上市公司所披露的信息需要能够影响市场对其公司未来获取预期现金流的期待。此种预期反映了资产所能带来经济利益的大小,

---

〔3〕《中共中央 国务院关于构建更加完善的要素市场化配置体制机制的意见》。

〔4〕天职国际:《2025年中报上市公司数据资产入表全景观察》,载新浪财经官网,https://finance.sina.com.cn/wm/2025-09-09/doc-infpwqyk5205516.shtml,2025年10月17日访问。

〔5〕参见徐文鸣、刘圣琦:《新〈证券法〉视域下信息披露"重大性"标准研究》,载《证券市场导报》2020年第9期。

也是投资者做出决策的重要依据。〔6〕在数据资产逐渐成为上市公司资产重要组成的情况下,上市公司的数据资产价值将是投资者做出投资决策的关注点。

在所有影响数据资产价值的因素中,网络安全一直被认为是制约上市公司数据资产价值判断的关键因素。〔7〕在《关于加强数据资产管理的指导意见》中明确提出要坚持的首要原则就是确保安全与合规利用相结合。若缺乏安全保障,数据资产价值将大打折扣,无法成为前述所称的公司“资产”。数据价值的发挥在于流转。完整的数据价值链包括:收集—聚合—分析—使用和货币化,这些环节相互衔接、循环往复,形成价值链闭环。〔8〕一旦发生网络安全事件,上市公司受到处罚,数据流通中断,从而阻碍数据价值链的形成,使得数据不满足“经济性”的资产要求。

从比较法上,网络安全已经得到了市场的回应。在最新的国际 ESG 投资指标增加了对上市公司网络安全治理的考察。〔9〕数据资产出现安全问题的外溢是严重的,不仅影响某一个上市公司自身,而且会沿着数据价值链传递至上市公司的供应商、合作伙伴,和用户群体。可见,上市公司的网络安全状况联结了公司与其利益相关方,数据资产安全已然是一个利益相关者问题。

因此,随着数字经济的发展,以及人工智能应用的普及,公司对网络安全风险管控的状况,能够向投资者传达出其未来能否应对网络安全风险,并在风险社会中创造出更高的价值的能力,成为数据资产价值反映的重要增量。

(二)解决网络安全代理问题的治理共识

1. 信义义务事后追责的困境

据世界经济论坛发布的报告,网络攻击已被列为全球第四大威胁,

---

〔6〕 参见汪其昌:《以正当规则激励股票市场功能发挥》,载《比较》2023 年第 4 期。

〔7〕 参见李闻一、荣梦杰、刘雨等:《企业数据资产价值形成的微观原理及其估值研究》,载《会计之友》2024 年第 23 期。

〔8〕 参见刘悦欣、夏杰长:《数据资产价值创造、估值挑战与应对策略》,载《江西社会科学》2022 年第 3 期。

〔9〕 增加了对上市公司网络安全治理的考察,该项下的信息包括相关董事会成员在委员会中的成员资格,该委员会负责监督高级行政级别的网络安全策略,并具有必要的领导层运作能力以及理解此类风险的战略技能。通过这种方式,可以评估网络安全风险是否被视为具有战略意义。

而且网络犯罪者有能力窃取“最安全”的数据,任何公司都不能独善其身。[10] 网络安全事件的发生将给上市公司股东带来多重冲击:首先是降低上市公司在资本市场的声誉,导致股票预期价值的负面反馈,直接影响投资者收益。[11] 例如,2022 年澳大利亚最大的医疗保险公司 Medibank 因数据泄露导致股价下跌 18%。[12] 2023 年英国半导体材料厂商 Morgan Advanced Material 披露其受到网络攻击,直接导致其股价下跌超 5%。[13] 另外,若上市公司泄露的数据侵害到用户的个人隐私,将引发对上市公司的诉讼,最终又会影响到上市公司股东的权益。例如,全球最大的家装零售商家得宝公司在 2014 年遭受网络攻击后泄露了近 4,000 万消费者支付卡信息,最终支付了 1,750 万美元的和解费。[14] 面对网络安全事件给投资者带来的损失,直接向公司的管理者追究违反信义义务的责任存在困境。

一是上市公司的网络安全无法保证“绝对安全”,即便未能避免数据泄露,也不能认为管理者未尽到应有的风险管理义务。网络安全风险的不可预知性,决定了上市公司无法完全杜绝网络安全事件的发生,网络安全状态只能处于“相对安全”而非“绝对安全”的状态。[15] 例如,在万豪酒店信息泄露案中,衡平法院驳回了对董事会的追责指控,因为他们“被定期告知网络安全风险和缓解措施,并提供了年度报告……且在履职中专门对网络风险进行了评估,并聘请了外部顾问改进和审计人员审计企业网络安全实践。而在有人向董事会报告危险信号后,管理层采

---

〔10〕 See Young, Sam, *Contemplating Corporate Disclosure Obligations Arising from Cybersecurity Breaches*, Journal of Corporation Law, Vol. 38, 2013.

〔11〕 参见张楠、马治国:《数据资产证券化探索的法律困境与解决路径》,载《重庆大学学报(社会科学版)》2024 年第 2 期。

〔12〕 《Medibank 敏感数据被盗　股值一天蒸发 18 亿》,载澳大利亚特别节目广播事业局中文官网,https://www.sbs.com.au/language/chinese/zh-hant/podcast-episode/all-medibank-customers-affected-by-hack/de4azceih,2025 年 10 月 17 日访问。

〔13〕 《因网络攻击造成近亿元损失,这家半导体厂商股价大跌》,载安全内参官网,https://www.secrss.com/articles/51692,2025 年 10 月 17 日访问。

〔14〕 In re Home Depot Sholder Derivative Litig., 223 F. Supp. 3d 1317 (N.D. Ga. 2016) (No. 1:15-CV-2999 TWT).

〔15〕 参见许可:《迈向“数字公司法”:一个理论前言》,载《上海政法学院学报(法治论丛)》2025 年第 1 期。

取了一些措施来纠正这些失败,尽管这些努力最终没有成功。"〔16〕可见,尽管网络安全事件给上市公司带来了严重的危机,但是若仅以网络安全事件发生的这一结果来追究上市公司董事的责任恐难实现。受制于商业判断规则对管理者的保护,公司管理层可以很容易地实现免责抗辩,其只需证明公司存在内部控制系统,且网络安全也只是商业判断的众多考量因素中的一个。〔17〕也有观点主张,可将管理者对网络安全风险的管理义务纳入忠实义务的范畴,以绕过商业判断规则对董事的保护。〔18〕问题在于,对违反忠实义务的追究,缺少善意是一个必要条件,而要证明管理者存在明显违背公司利益行事的故意动机和行为将会非常困难。〔19〕

二是规范层面错位使得投资者在追责时缺乏清晰的法律依据。有学者总结,新《中华人民共和国公司法》系统性扩张了董事的义务,不仅强调了基本的合规义务,还在传统的忠实义务和勤勉义务之外构建了特别义务,如公司在结算时的清算义务。〔20〕而网络安全保障义务并未被单独规范或者置于勤勉忠实义务体系中。另外,虽然自2016年《中华人民共和国网络安全法》出台以来,我国相继颁布了《中华人民共和国个人信息保护法》《中华人民共和国数据安全法》(以下简称《数据安全法》),建立了对上市公司进行网络安全管控的法律体系,但其中的多数内容都仅停留在组织层面,未能落实到管理者的具体行为层面。例如,《数据安全法》中所规定的安全保障义务主体"数据安全负责人和管理机构"与公司管理主体无法一一对应,此种主体的模糊性带来的问题便是对公司管理者施加责任的困难。〔21〕

2. 信息披露的事前解决路径

面对直接以违反信义义务追究董事责任的困境,利用信息披露制

---

〔16〕 Firemen's Retirement System of St. Louis on Behalf of Marriott International, Inc. v. Arne M. Sorenson, 2021 WL 4593777, at *2 (Del. Ch. Ct. Oct. 5, 2021).

〔17〕 See Victoria C. Wong, *Cybersecurity, Risk Management, and How Boards Can Effectively Fulfill Their Monitoring Role*, UC Davis Business Law Journal, Vol. 15, 2015.

〔18〕 See H. Justin Pace, *Rogue Corporations: Unlawful Corporate Conduct and Fiduciary Duty*, Missouri Law Review, Vol. 85, 2020.

〔19〕 Stone v. Ritter 911 A. 2d 362(2006).

〔20〕 参见邹海林:《公司法上的董事义务及其责任配置》,载《法律适用》2024年第2期。

〔21〕 参见陈洪磊:《论公司董事的数据安全保障义务》,载《当代法学》2025年第2期。

度,通过自证清白的方式促使上市公司的管理者关注网络安全风险,并对违反者施以虚假陈述责任成为更优的路径。一方面,信息披露制度并未否定上市公司管理者在网络安全问题上应尽到的信义义务,而是通过具体的披露指标和披露程序使得对董事的追责更具操作性。另一方面,信息披露是一种事前预防手段,更加契合网络安全风险管理的预防性要求。实际上,这一做法得到了世界范围内许多监管者的支持。例如,美国 SEC 要求所有在美国上市的公司都要披露网络安全事件信息和网络安全治理信息。〔22〕 澳大利亚更新了其信息披露规则,也要求上市公司披露数据泄露事件的有关信息。〔23〕 欧盟在其《通用数据保护条例》中规定,公司发生数据泄露后必须在 72 小时内向数据保护机构报告事件。〔24〕 我国监管机构同样注意到了上市公司网络安全风险治理的重要性,已经尝试通过信息披露的方式改善上市公司的网络安全风险治理状况。深交所和上交所发布的上市业务审核指南中都设置了针对"数据安全和个人信息保护"的核查要点,深交所还更新了行业信息披露自律指引,鼓励部分行业的上市公司持续披露与网络安全状况有关的信息。

综上,上市公司的网络安全不仅与数字时代的上市公司价值评价息息相关,还催生了上市公司的投资者与管理者之间新的"委托—代理"难题。利用信息披露制度,要求上市公司的管理者披露上市公司网络安全治理状况,一方面可以帮助投资者对上市公司数据资产的价值作出判断,另一方面也为投资者追究高管虚假陈述责任提供了依据。

二、网络安全强制披露优于自愿披露的证成

网络安全风险的反噬效应与负外部性使实践中的自愿披露机制出现披露不足和系统性风险的市场失灵问题。相比之下,强制披露通过统一标准与制度化安排,更有利于保护投资者权益,并维护资本市场秩序。

〔22〕 17 CFR Parts 229, 232, 239, 240, and 249.

〔23〕 Australian Securities Exchange, Continuous Disclosure: Listing Rules 3.1 - 3.1B.

〔24〕 General Data Protection Regulation.

（一）强制披露应对网络安全自愿披露供给不足的优势

1. 网络安全的反噬效应引发自愿披露的供给不足

网络安全自愿披露所产生的信息供给不足原因在于信号传递逻辑难以适配网络安全信息的披露。自愿信息披露的作用机理源自经济学中的信号理论（Signaling Theory），该理论认为，发行人可以通过向市场披露对手公司所没有的特异信息以获得市场的青睐。〔25〕这一信号传递机制在网络安全问题上无法发挥出应有的作用。一方面，网络安全信息不同于财务信息，其存在披露的“反噬”效应，主动披露的内容可能会被利用，作为攻击上市公司自身的地图，换言之，披露会增加上市公司自身的风险。例如，上市公司发生网络安全事件后，若在漏洞尚未完全修复前即披露网络安全事件的漏洞，往往会诱发二次攻击。〔26〕

另一方面，即便上市公司所披露的信息经过了风险审查降低了“反噬”风险，但此种披露很可能会向公众传达出自身脆弱，极易受到攻击的信号，进而会增加高管被起诉的风险。〔27〕尽管目前实践中未有因网络安全事件的发生而被以违反信义义务追责的管理者，但是股东衍生诉讼所传递出的负面消息，仍然能够通过经理人市场的信誉机制使得管理者利益受损。〔28〕由此，面对网络安全信息披露可能带来“言多必失”的后果，公司的管理者显然会倾向于减少网络安全相关信息的披露，甚至隐瞒公司网络安全的真实状态。例如，2017 年美国知名征信机构 Equifax 公司因遭到网络攻击泄露了近 1.43 亿的个人信息，导致此股价累计跌幅达 30%，市值蒸发超 50 亿。而在网络安全事件发生后，公司的三名高管隐瞒信息，并提前抛售了所持的价值近 200 万美元的股票。

因此，由于网络安全信息的反噬效应，自愿披露在网络安全问题上不仅难以发挥信号作用，反而带来信息供给不足的市场失灵问题，最终

---

〔25〕 参见谭劲松、宋顺林、吴立扬：《公司透明度的决定因素——基于代理理论和信号理论的经验研究》，载《会计研究》2010 年第 4 期。

〔26〕 参见黄道丽：《网络安全漏洞披露规则及其体系设计》，载《暨南学报（哲学社会科学版）》2018 年第 1 期。

〔27〕 See Rebecca Rabinowitz, *From Securities to Cybersecurity: The SEC Zeroes in on Cybersecurity*, Boston College Law Review, vol. 61, 2020.

〔28〕 See James D. Cox, *The Social Meaning of Shareholder Suits*, Brooklyn Law Review, vol. 65, 1999.

损害投资者的利益。

2. 以强制披露的统一性回应供给不足的难题

强制披露与自愿披露是强制与自由这对关系在资本市场中的体现。作为国家介入自由市场的一种手段,其必要性在于实现资本市场的资金配置效率。此种资金配置效率的考察因素包括投资者的决策效益和上市公司的披露成本。

资本市场的信息不对称地位是一直存在的,即便是强制披露亦无法解决资本市场的信息不对称。强制披露的作用不在于对投资者需要哪些信息进行招投标,而是通过统一的标准实现信息的可比性;换言之,强制信息披露制度的作用不在于扩大信息的总量(分母),而在于提高信息可供获得者的数量(分子)。具体而言,强制信息披露制度可通过标准化的披露要求,固定上市公司的披露,包括披露内容、披露位置、披露频次等等,进而实现信息的可比性,以供不同的投资者在设定的披露框架下做出决策。

另外,强制信息披露可以通过对披露的适用范围和披露内容做差异化安排控制上市公司的披露成本。差异化的信息披露设计并不违反强制披露的基本原则,且已经成为通行做法,常见的路径包括分行业、分规模、分板块的信息披露。这些差异化安排能够实现对不同上市公司披露成本的考量,尤其对网络安全而言,因不同行业的上市公司所带来的社会影响不同,在网络安全风险控制的成本投入存在明显差异。即便在同一行业内,不同规模的上市公司发生网络安全事件所带来的影响也是不同的,大规模的上市公司由于用户基数大、业务链条长,网络安全事件更易产生广泛的影响,其在网络安全风险控制上的投入更高。由此,根据不同公司网络安全风险的实际情况做出差异化的强制披露安排,可以避免"一刀切"的制度弊端。

(二)强制披露应对网络安全自愿披露外部性的优势

除了能够解决网络安全披露在自愿披露下所出现的信息供给不足的市场失灵外,引入标准化的强制披露的另一理由在于强制披露本身能够内化上市公司网络安全风险的外部性问题,防止市场出现系统性风险。

1. 网络安全存在负外部性的固有风险

上市公司的网络安全问题是数字经济时代风险的典型,其具有明显

的外溢性,关涉利益主体众多,超出了传统的公司治理范畴。对于上市公司而言,其网络安全风险治理的优劣不仅关乎自身安全,更会通过供应链扩散,影响到整个产业链条的上下游公司。〔29〕 例如,2020 年 SolarWinds 网络安全事件,SolarWinds 公司的软件更新包被植入了恶意软件,并通过该公司的 Orion 平台扩散,影响了与该公司有合作关系的政府部门、关键基础设施及多家美国上市的 500 强企业。再如,2024 年微软公司受网络安全供应商 CrowdStrike 更新推送影响,导致 Windows 系统蓝屏,影响了全球数百万的电脑系统。这些案例表明,网络安全风险远超单一公司的内部治理范畴,已经成为威胁市场稳定的公共问题。

另外,网络安全事件的爆发存在潜伏期。许多数据泄露事件的发生并非由上市公司自身,这加剧了风险外溢的强度。雅虎公司数据泄露案即是典型,该公司的数据泄露发生于 2014 年,而直到 2016 年泄露问题才得以被发现并披露,最终影响了 30 亿个用户的账号安全。IBM(International Business Machines Corporation)《2024 年度数据泄露成本报告》显示,只有 42%的数据泄露事件是由公司自己的安全团队发现,34%的泄露事件是由良性第三方机构披露,24%的泄露事件由网络攻击者自身披露。

可见,上市公司的网络安全治理关涉多方利益主体。而自愿披露下,上市公司倾向于报告自身的特异信息,以期获得融资机会,对可能影响其他主体的信息并不关心,这些信息对公司而言是非必要的成本。

2. 强制披露内化网络安全风险的经验

回顾美国法在上市公司披露网络安全问题上的立法经验,印证了自愿披露在解决网络安全外部性问题的不足。美国 SEC 在 2011 年发布的最初的网络安全披露文件——《网络安全披露指引》(*Disclosure Guidance: Topic No.2 Cybersecurity*),仅关注上市公司的网络安全事件,并且不强制要求上市公司披露有关信息。〔30〕 尽管该指引的初衷是引导上市公司规范披露信息,但后续频发的网络安全事件,凸显出这一指引的不足。

---

〔29〕 参见周圣:《证券市场网络风险的法律规制研究——以国际实践系发展为视角》,载《证券市场导报》2020 年第 6 期。

〔30〕 See Matthew F. Ferraro, *Groundbreaking or Broken*; *An Analysis of SEC Cybersecurity Disclosure Guidance*, *Its Effectiveness*, *and Implications*, Albany Law Review, Vol. 77, 2013.

随后,SEC 在 2018 年扩大了 2011 年指导原则的范围,发布了新的文件《关于上市公司网络安全信息披露的声明和指导意见》(*Commission Statement and Guidance on Public Company Cybersecurity Disclosure*)。该意见关注网络安全管理的过程和政策,但仍采取自愿披露的态度,未能规制上市公司在网络安全问题上的虚假披露现象。接连发生的两起网络安全虚假陈述案件即是例证:2021 年房地产结算服务公司 First American Financial Corporation 因暴露客户敏感信息的网络安全漏洞违反披露控制和程序被 SEC 做出 48.7 万美元的罚款。[31] 同年,皮尔森公司因在披露的信息中隐瞒关于公司严重的网络安全漏洞而被 SEC 做出 100 万美元的罚款。[32]

最终,为有效改善美国资本市场各主体的网络安全,保护股东及投资人的利益,经过一年多的征求意见后,SEC 发布了最新的文件《上市公司网络安全风险管理、战略、治理和事件信息披露》(*Cybersecurity Risk Management*, *Strategy*, *Governance*, *and Incident Disclosure*)。该规则强制要求所有在美国上市的公司披露网络安全信息,还从上市公司风险管理和战略、上市公司治理、网络安全事件三方面进行了全方位的披露要求。[33] 这一转向表明,只有强制披露才能真正迫使企业全面报告风险,从而内化外部性,维护市场稳定。

综上,自愿披露因反噬效应导致信息供给不足;又因网络安全风险的外溢性,难以保护更广泛的投资者和利益相关方。相比之下,强制披露通过标准化的制度安排,可以缓解自愿机制导致的市场失灵,确保投资者决策的透明性与资本市场的稳定性。当然,强制披露的引入需要注意上市公司合规成本问题,应采取审慎态度,通过差异化的制度安排提升制度带来的效益。

---

〔31〕《美国证券交易委员会指控发行人网络安全披露控制失败》,载美国证券交易委员会官网,https://www.sec.gov/news/press-release/2021-102,2025 年 10 月 17 日访问。

〔32〕《美国证券交易委员会指控皮尔森公司在网络漏洞方面误导投资者》,载美国证券交易委员会官网,https://www.sec.gov/news/press-release/2021-154,2025 年 10 月 17 日访问。

〔33〕同前注〔22〕。

三、上市公司强制披露网络安全的制度回应

（一）网络安全强制披露的内容边界

《中华人民共和国证券法》（以下简称《证券法》）规定了证券的发行、交易的三大原则，公开、公平、公正原则。公开原则是其中的首要原则，在信息披露领域即体现为公开主义。信息工具作为一种柔性监管工具，其实效的发挥需要信息能够公开。而网络安全强制披露需要关注的第一个特殊问题是哪些信息应予公开披露。实践中自律披露指引所规定的信息显然是零散的、不充足的，需要在借鉴国际标准的基础上，形成体系化的披露内容。当然，需要先明确当前的“重大性”标准并不构成对网络安全信息披露内容的阻碍。

1. “重大性”标准的重塑

根据我国《证券法》的规定，信息披露的“重大性”标准散见于发行申请文件、内幕信息、应予报告事项、自愿披露事项。分别表述为：“投资者作出价值判断和投资决策所必需的”“经营、财务或者对该发行人证券的市场价格有重大影响的”“股票交易价格产生较大影响的”“与投资者作出价值判断和投资决策有关的”。由此，我国《证券法》规定了“价格测试”与“投资者决策测试”的二元标准。就这二者之间的关系，有学者认为“价格测试”作为定量测试优先适用，而“投资者决策测试”作为定性标准兜底适用。〔34〕 也有观点认为，“价格测试”与“投资者决策测试”二元并存的标准是核准制向注册制改革未尽完成的产物，二者之间的关系是特殊与一般的关系。〔35〕 还有学者指出“价格测试”与“投资者决策测试”不过是对上市公司应该披露哪些内容这一个问题分别从客观和主观层面作出的回答，实质上是一个标准。〔36〕 尽管上述观点各有侧

〔34〕 同前注〔5〕。

〔35〕 参见马志健：《注册制背景下信息披露重大性标准探究》，载《财会月刊》2022 年第 8 期。

〔36〕 参见曾洋：《证券法信息披露规则的体系解释》，载《南大法学》2024 年第 1 期。

重,但无一例外都认可“投资者决策测试”在资本市场注册制改革后应对日益复杂的披露内容上的重要作用。可以说,对于哪些信息应予强制披露,价格测试只不过给出了一种客观的、较为简便的判断标准,但实践中存在很多披露的内容并不符合价格测试同样予以了披露,典型的例子是“管理层讨论与分析”中的内容。对此,有学者认为这是缘于“投资者决策测试”中投资者画像顺应时代发生了变化。〔37〕 当然,这并不是意味着投资者不关注价格,相反,这反映出投资者对上市公司价值判断点从一维走向多维。就这一点而言,随着投资者关注点的变化,“重大性”的标准必然会发生变化。

实际上,从“重大性”标准的发展历程来看,理性投资者的画像是随着案例的推动而不断得到进化。例如,在 TSC Industries, Inc. v. Northway, Inc.一案中,美国最高法院首次确立了“理性投资者标准”,认为重大性是指“合理投资者认为重要的信息”,信息是否重大取决于其是否会在理性投资者的决策中“总体上被考虑”;在 Basic, Inc. v. Levinson 一案中,法院进一步将预测性信息(即未来可能性事件)纳入重大性判断范围,强调市场对潜在未来事件的反应也构成重大信息;在 Matrixx Initiatives, Inc. v. Siracusano 一案中,法院认为即使缺乏统计显著性,只要信息可能对投资者决策产生重要影响,也应认定为重大信息。〔38〕 从美国“重大性”标准的发展中可以看出,因应投资者决策的关注,信息披露的“重大性”标准已经从单纯的股价敏感性扩展至服务投资者预期和反映公司治理相关的信息。

在当前网络安全监管趋向严格和公众对数据安全高度敏感的背景下,影响上市公司价值的因素除了网络安全由外向内给公司带来的财务影响外,更重要的是包括公司网络安全由内向外给用户、其他公司,甚至整个市场的影响。这种对内的财务影响和对外的社会影响之间并不存

〔37〕 参见楼秋然:《ESG 信息披露:法理反思与制度建构》,载《证券市场导报》2023 年第 3 期。

〔38〕 TSC Industries, Inc. v. Northway, Inc., 426 U. S. 438 (1976)、Basic, Inc. v. Levinson, 485 U.S. 224 (1988)、Matrixx Initiatives, Inc. v. Siracusano, 563 U.S. 27 (2011).

在明晰的界限,实际上,社会影响往往最终也会转化为财务影响。〔39〕遭受网络安全攻击一定程度上的过错并不在公司管理者,但是面对网络安全问题不采取应对措施,造成社会危害,则会给上市公司应对风险的能力带来负面评价,公司估值自然一落千丈。例如,美国知名征信机构Equifax公司在遭受网络攻击后,因应对迟缓,股价大跌30%,市值蒸发超50亿美元。相反,同一时期的美国国家第二大医疗保险公司Anthem公司也发生了网络安全事件,但Anthem公司主动及时提醒其客户公司,并披露泄露情况,同时还披露了其所采取的应对泄露的行动,包括配合联邦调查局展开合作调查,聘请网络安全公司审查其系统漏洞,结果是Anthem公司股价仅下跌1.1%。〔40〕这两则案例的对比充分表明,即使网络安全事件不可能完全避免,公司披露网络安全的及时性与网络安全风险治理的积极性,才是投资者对公司价值作出评价的关键依据。

因此,上市公司披露网络安全信息的重大性边界除了根据"价格测试标准"在评估数据泄露对公司造成的损失的基础上直接划定披露网络安全事件外,还应通过解释"投资者决策测试"间接增加能够反映公司网络安全举措对外产生影响的非财务信息。

2. 国际披露规则的结构性借鉴

上市公司的网络安全会产生哪些可供披露的信息不仅是一个管理问题,更涉及上市公司的治理层面的内容,是上市公司的治理与技术管控融合的产物。对此,可以借鉴有关上市公司网络安全的国际标准,总结其在网络安全风险管理方面的成功经验,为网络安全强制披露的内容提供结构性基础。

通行的网络安全标准有NIST网络安全框架(以下简称"CSF框架")和ISO/IEC 27000系列标准(以下简称"ISO/IEC标准")。这两个标准都旨在通过帮助组织建立并实施网络安全管理制度来确保组织能保护其信息资产和利益,前者侧重于治理与风险管理的宏观框架,后者

〔39〕 Mitrović Milena, *Materiality Concept(s) in the EU Sustainability (Non-Financial) Reporting: The Challenge of Equivalence*, https://ssrn.com/abstract=5070736, visited May 2024.

〔40〕 See Paul Ferrillo, *To Overdisclose or Not: That Is the Question with Cybersecurity*, Florida State University Business Review, Vol. 20, 2021.

强调控制措施的细化。CSF 框架最新的 2.0 版本(以下简称“CSF2.0”)的核心部分(Core)包括了六大关键功能:治理、识别、保护、检测、响应、恢复;其中,网络安全治理是其他五个功能的核心,公司的管理者应予以关注网络安全并采取措施实施网络安全风险管控。核心中的六大功能从网络安全管理的结果角度给予了公司参考,但在具体的措施上并未提供具体的路径。

表 1　CSF 框架内容

功能	类　　别
治理	1. 组织环境;2. 风险管理战略;3. 角色、职责、权限;4. 政策;5. 监督;6. 供应链风险管理
识别	1. 资产管理;2. 风险评估;3. 改进
保护	1. 身份管理、认证、访问控制;2. 安全意识与培养
检测	1. 持续监控;2. 不良事件分析
响应	1. 安全事件管理;2. 安全事件分析;3. 安全事件响应与沟通;4. 安全事件遏制
恢复	1. 安全事件恢复计划执行;2. 安全事件恢复沟通

相比之下 ISO/IEC 标准则更为具体地列举了公司在进行网络安全管理中应实施的步骤。2022 年更新的 ISO/IEC 标准分别从组织环境、领导、规划、支持、运行、绩效评价、改进七个方面给出了组织在建立、实施、维护和持续改进信息安全管理体系的要求,并在附录中列举了组织控制、人员控制、物理控制、技术控制四个控制标准及项下的 93 个小项。

表 2　ISO/IEC 27001 内容

控制项目	控　制　内　容
组织环境	1. 理解组织及其环境;2. 理解相关方的需求和期望;3. 确定信息安全管理体系范围;4. 信息安全管理体系

续表

控制项目	控　制　内　容
领 导	1. 领导和承诺;2. 方针;3. 组织的角色,责任和权限
规 划	1. 应对风险和机会的措施;2. 信息安全目标及其实现规划;3. 变更规划
支 持	1. 资源;2. 能力;3. 意识;4. 沟通;5. 文件化信息
运 行	1. 运行规划和控制;2. 信息安全风险评估;3. 信息安全风险处置
绩效评价	1. 监视、测量、分析和评价;2. 内部审核;3. 管理评审
改 进	1. 持续改进;2. 不符合及纠正措施

从网络安全强制信息披露制度应予构建的内容来看,尽管两个标准侧重不同,但都给出了以下启示:一是应当确立治理机制作为披露的核心内容。例如,CSF2.0 中网络安全治理被设定为独立的功能区,ISO/IEC 27001 则强调企业领导层对信息安全管理体系应承担责任。这一变化已经得到了立法的响应,美国 SEC 在 2023 年出台的最新规则中明确将网络安全治理信息独立于网络安全事件予以披露。二是应当强化披露的过程性。例如,CSF2.0 中构建了“检测—响应—恢复”循环,ISO/IEC 27001 在“改进”部分强调持续改建。对资本市场而言,这种动态更新机制能让投资者及时掌握风险的演变情况,从而缓解时效性与风险变化之间的矛盾。

3. 披露内容的具体指向

在借鉴国际标准的基础上,本文认为,上市公司网络安全信息披露至少应当包括两个基本层面内容:网络安全事件信息和网络安全治理信息,前者回应投资者对即时风险的关切,后者回应投资者对企业长期稳健运行的期待。同时,信息披露制度还需要回应网络安全所面临的透明性与安全性之间的平衡。因为网络安全信息本身具有高度的敏感性,披露得越详细,越可能会给潜在的攻击者提供具体的路线图(road map),增加上市公司的成本。这要求披露内容设计坚持“重影响、轻细

节”的原则。

(1) 网络安全事件的信息

网络安全事件披露目的在于告诉社会公众采取措施及时止损,具体制度设计中需注重影响披露,减轻细节披露,以免遭受二次攻击。

首先,披露网络安全事件的基本信息,包括发生时间,持续时间及产生风险的源头。比较法上,美国证券交易委员会(SEC)在2023年通过的最终规则要求上市公司披露重大网络安全事件的相关信息,但明确无需涉及具体技术细节。[41] 此种规定存在的风险是上市公司可能会以细节为由模糊处理,逃避披露。对此,应根据网络安全攻击的不同阶段采取不同的披露程度设计。初次遭遇网络攻击时,上市公司应披露一些基本信息,表明事件的性质和初步影响,同时向投资者提供必要的透明度;随着事件的调查进展,上市公司应当逐步更新信息,以确保投资者能够实时掌握风险变化。

其次,在表达披露内容时应呈现出网络安全事件所带来的多元影响,不仅包括网络安全事件给公司相关业务、财务和战略带来的影响,还应包括给用户、市场带来的影响。从风险的响应和恢复角度,披露的具体内容应包括事件发生后所采取的即时补救措施,以及未来应对的长期措施,而非沉溺于技术性的描述。

最后,还需要关注两种特殊情况。一是如果公司在一定时间内,连续发生多起小规模的网络安全泄露,是否需要披露?二是上市公司如果在遭受勒索后已经支付了赎金,且数据得到了归还,未造成泄露的严重后果,是否需要披露?对此,应区分情况讨论。就第一种情况,如果不断出现的小规模攻击是因为上市公司存在网络安全漏洞,且该漏洞无法在短时间内解决,甚至在不断扩大,则需要披露,以便告知用户和其他公司提前做好防范。具体而言:需要披露这些事件之间存在的关联性,并作出系统性风险的提示。就第二种情况,若支付赎金是因为公司泄露数据庞大,为了保护敏感数据而支付赎金,则需要披露,并表明事件的决策。但如果漏洞是可控的,泄露的数据也只是一小部分,支付赎金是最优的解决办法,则无需披露,以免增加公司的披露成本。

---

〔41〕 同前注〔22〕。

（2）网络安全风险治理的信息

网络安全风险治理信息的披露旨在揭示上市公司在日常经营中是否建立了系统性、可验证的风险管理机制。这些信息主要指向上市公司的风险控制系统，其逻辑为，公司中有哪些主体、通过什么样的方式、控制哪些风险，以及控制风险的效果如何。对此，结合“识别”“检测”“保护”的三大内容，上市公司应予披露的信息包括：风险管控的主体、流程、第三方参与，披露的形式采取定期披露文件，每年或者每半年披露。

其一，上市公司负责风险管控的主体。董事会作为上市公司的治理中心，对网络安全风险管理负有监督职责，公司治理的披露即围绕董事会对网络安全的监督职责展开。上市公司首先应披露董事会是否下设了专门的网络安全风险管理委员会或者专门的人员。

其二，上市公司进行风险识别的流程。这一流程指向董事会是否建立了通畅的网络安全风险信息传递机制。对于公司的风险管理而言，畅通的董事、经理、执行层、员工之间的信息传递渠道是进行风险监督和反馈的必要条件。〔42〕 通过信息传递机制可以实现董事对风险的及时识别与判断。

其三，上市公司网络安全预防中的第三方参与信息。考虑到实践中网络安全事件时常出现由第三方主体引发的情况，因而需要上市公司披露其网络安全风险管理过程中是否存在如外部评估师、顾问、审计师或者其他第三方参与的情况。

表 3　上市公司网络安全强制披露信息内容

一 级 事 项	二 级 事 项	三 级 事 项
网络安全事件	事件基础信息	发生及持续时间
		攻击类型
		攻击入口

〔42〕 参见吴越、陈杰：《董事监督义务裁量规则研究》，载《社会科学研究》2023 年第 6 期。

续表

一级事项	二级事项	三级事项
网络安全事件	事件影响范围	用户影响
		业务影响
		财务影响
	事件响应措施	即时措施
		长期措施
网络安全治理	治理架构	董事会专门委员会
		首席信息安全官
	风险识别机制	威胁情报来源
		风险评估流程
	供应链风险管理	关键第三方清单
		供应商安全审计标准
特殊场景补充	多次小规模事件	事件关联性
		系统性风险提示
	赎金支付事件	决策依据
		漏洞修复情况

4. 披露内容的例外设置

当然,并非所有的网络安全事件都要披露,对于披露的内容涉及国家安全、商业秘密、个人隐私等高度敏感的信息,则应当允许暂缓或豁免披露。

比较法上,澳大利亚在 2024 年 6 月更新后的信息披露第 8 号指引中,专门设置了网络安全事件信息的豁免披露的规则。数据泄露涉及商业秘密(Trade secret)需要证券交易所进行机密信息判断与理性人判断,

若符合机密且一般人都不希望该信息披露,则豁免披露。〔43〕

证监会2025年4月发布了《上市公司信息披露暂缓与豁免管理规定》(以下简称《管理规定》,2025年7月1日起施行),在制度逻辑上与澳大利亚的做法异曲同工,为网络安全信息披露的例外制度设计提供了直接参照。根据《管理规定》,暂缓或豁免的事由必须有确凿证据支撑,且限于披露会害及国家安全、公司、客户、供应商和个人隐私的高度敏感信息。而且,《管理规定》施加了严格的程序控制,暂缓或豁免必须履行内部审核和董事会审议程序,由董事长与董事会秘书负责登记备案并留档十年以上。另外,暂缓或豁免披露并非永久不披露,一旦豁免理由消除,或信息泄露、市场出现传闻,则公司必须及时补充披露,并说明理由、程序及暂缓期间知情人交易情况。

可见,无论是澳大利亚的最新披露指引,还是我国《管理规定》,二者在制度逻辑上是共通的,都是通过设计暂缓或者豁免的内容和程序安排对网络安全信息的披露例外制度作出控制。此种制度安排能够回应网络安全信息披露的敏感性,在最大程度保证信息披露透明度的基础上,避免过度披露细节可能带来的次生损害。因此,网络安全信息的豁免披露安排,不应被理解为对透明度要求的削弱,而是立足于审慎披露的逻辑基础上所作出的"必要例外"。

(二)网络安全强制披露适用范围的差异化

1. 基于成本收益考量的差异化基础

高效的强制信息披露制度一定是考虑了披露的收益与成本,避免浪费或对公司的过度监管。〔44〕利用强制信息披露制度需要考虑两类成本,上市公司的合规成本和监管者的监管成本。

网络安全强制披露制度的适用范围设计,必须充分重视上市公司的合规成本差异。与其他信息相比,网络安全强制披露带给不同公司的合规成本差异将是极为明显的。因为不同的上市公司所面临的网络安全风险程度是差异化的,公司所预期投入的成本自然是不同的。例如,互

〔43〕 同前注〔23〕。

〔44〕 See Frank H. Easterbrook & Daniel R. Fischel, *Mandatory Disclosure and the Protection of Investors*, Virginia Law Review, Vol. 70, 1984.

联网平台公司、云计算服务提供商、网络安全服务公司通常会因存储大量用户数据而面临极高的网络攻击风险。另外,前述公司的上下游公司在业务模式、数据资源储备、系统架构等也有所不同,它们在面临网络攻击时的脆弱性和风险敞口也存在巨大差异。〔45〕 IANS(Intel Advanced Network Service)发布的《2023 年网络安全预算基准摘要报告》显示,2023 年企业的网络安全预算占 IT 总预算的平均值为 11.6%,其中科技行业、消费品和服务行业的网络安全预算支出占 IT 总预算均超过 15%,而制造业、医疗、零售的支出都在 8.2%以内。若统一要求所有上市公司在网络安全问题上适用同一强制披露,显然违背了成本与收益相称原则,将徒增网络安全较低上市公司的合规成本,影响公司的资源配置,最终害及公司投资者利益。

此外,无差别的施加强制披露也会增加监管成本。研究表明,《萨班斯-奥克斯利法案》直接向高管施加合规压力的方式并未取得预期效果,未能阻止规避行为和寻租的发生,因为此种改革并没有给公司带来多少利润,高管没有多少动力配合改革。〔46〕 然而,因为该法案无差别地针对所有公司施加了审计要求,增加了监管成本,监管者不得不投入资源监控众多的中小公司。而这又加重了中小公司的审计成本,打击了这些公司参与资本市场和上市的积极性。

因此,差异化的披露安排越来越得到监管者的青睐。针对实践中不同行业、不同规模、不同板块的上市公司在网络安全披露上成本与收益的差异,本文据此提出区分行业、规模、板块的差异化安排。

2. 差异化适用的具体安排

(1) 区分上市公司所在行业

结合我国当前网络安全风险存在行业突出的现状,强制披露的适用范围应当先聚焦于平台型上市公司及其供应链企业。所谓平台型上市公司,是指以数据为核心生产要素、直接提供互联网平台、云计算、金融科技或网络安全服务的上市公司。与传统行业相比,平台型上市公司与

〔45〕 参见洪延青:《"以管理为基础的规制"——对网络运营者安全保护义务的重构》,载《环球法律评论》2016 年第 4 期。

〔46〕 参见叶德珠、蔡赟:《高管人员信息披露造假的行为经济学分析》,载《财经科学》2008 年第 1 期。

消费者、用户、供应商之间的关系较传统上市公司而言更为密切,是公司治理中“利益相关者主义”的典型体现。[47] 在数字时代,平台公司已成为人类生活的中心场域,其不仅是基础设施的提供者,更是数据的控制者,其网络安全水平直接关乎公共利益乃至证券市场的系统性风险。[48] 欧盟《数字运营弹性法案》(*Digital Operational Resilience Act*)的颁布正是对金融平台公司网络安全的回应,也着力于提升整个欧盟金融系统的网络韧性和运营安全。因此,要求平台型上市公司适用网络安全强制披露制度具备制度可行性。

同时,供应链企业的安全漏洞往往是平台公司网络安全风险的触发点。最典型的案件便是 Target 公司数据泄露事件。作为美国知名零售商,Target 公司数据泄露的源头是其通暖供应公司,攻击者在获得了该通暖供应公司的网络访问权限后便对 Target 公司的网络进行渗透,并在支付系统中植入了恶意软件,最终影响了 4,000 万张信用卡和 7,000 万个客户账户。可见,供应链公司的漏洞会导致平台公司风险外溢,所以也必须纳入披露体系,但考虑到其业务性质和合规成本,披露要求可限制在二级事项范围,不予以细化,具体内容可根据公司而定,以平衡风险防范与成本约束。

(2) 区分上市公司的规模

网络安全信息的强制披露会加剧规模较小的上市公司的负担,根据规模不同采取差异化的披露是合乎成本收益的考量。信息披露成本在大中小型公司之间并无显著差别,但对规模较小的上市公司而言,却可能成为沉重负担。[49]

比较法上,欧盟《可持续发展指令》(*Corporate Sustainability Reporting Directive*)就对大规模企业和小规模企业做了差异化的区分。美国 SEC 自 1992 年始便通过 S-B 规则对融资金额少或者规模较小的上市公司采取了差异化的披露规则,后在 2008 年提升了判断小公司的销售额或

〔47〕 同前注〔15〕。

〔48〕 参见邹青松:《国家介入超级平台公司的法理基础与制度建构》,载《法商研究》2024 年第 1 期。

〔49〕 参见徐聪:《试论我国上市公司差异化信息披露制度之构建》,载张育军、徐明主编:《证券法苑》(第 4 卷),法律出版社 2011 年版。

者流通股市值标准,并进一步增设了较小规模公司和新型成长公司。[50]在我国,上市公司的规模作为差异化披露的重要指标已经得到了理论界的支持。有研究将这一规模指标进一步细化为公司的盈利能力、偿债能力、营运能力、分红能力、资本结构等因素,并结合公司治理等其他因素对上市公司进行画像。[51]

因此,若统一要求不同规模的公司强制披露网络安全信息显然会加重规模较小的上市公司的负担。故本文建议在参考如盈利能力、偿债能力、成长能力等指标的基础上区分大型上市公司,并做强制披露要求。

(3)区分上市公司所处板块

通过多层次的证券市场划分,能够将风险不同的上市公司和投资者相匹配。这意味着信息披露的内容在不同板块所能取得的边际收益是不同的。在不同的市场中,投资者对待诸如网络安全、社会责任、环境信息的态度并不相同。已有研究表明,主板市场的投资者对诸如社会责任等非财务信息敏感度更高,上市公司的披露往往会获得市场的正向反馈,从而提升公司的声誉与股价表现;而在中小板市场中,投资者对上市公司披露的社会责任信息反映并不强烈,以至于社会责任报告的详细程度与投资者反馈趋向于负相关。[52]

在构建网络安全信息制度的适用范围时,同样需要考虑此类非财务信息在不同板块市场披露所能获得的边际收益。因此,本文建议考虑在主板市场优先建立网络安全强制披露制度,而对创业板、中小板市场则采取适度或分阶段实施的模式,保持了制度的审慎与渐进性。

四、结论

数据在成为上市公司重要资产的同时,也成为投资者关注的重点,

---

〔50〕 参见朱嘉诚:《科创板视野下我国差异化信息披露制度构建的进与退》,载《财经法学》2019 年第 3 期。

〔51〕 参见徐静、袁慧:《基于 RFM 模型的上市公司违规行为画像研究》,载《数据与计算发展前沿》2023 年第 6 期。

〔52〕 参见王诗雨、汪官镇、陈志斌:《企业社会责任披露与投资者响应——基于多层次资本市场的研究》,载《南开管理评论》2019 年第 1 期。

但因网络安全问题上的信息不对称使得投资者难以行使股东权利;无论是表决、转售、诉讼都需要上市公司的管理层披露网络安全方面的信息。强制披露不仅能解决自愿披露所存在的供给不足难题,且能应对网络安全存在的外部性问题。但同时,网络安全强制披露制度的设计必须考虑到给上市公司带来的合规成本增加。对此,在制度设计层面,应当在披露内容与适用范围两个核心问题上遵循最小必要与差异化适用的原则。在内容上,通过设置应予披露的事项和披露例外事项来划定披露的内容边界;在适用范围上,通过区分不同行业、规模、板块的上市公司,作出差异化的强制披露制度适用范围。

(编辑:沈卓韵　高鹏程)