网络风险评估与资本管理

研究成果：Cyber Risk Assessment for Capital Management
作者：Wing Fung Chong，**冯润桓**，胡兆轩，张临风
发表期刊：*Journal of Risk and Insurance,* 2025, 92(2), 424-471

在数字化和信息技术高度依赖的时代，网络攻击、数据泄露等事件频发，企业面临巨大的运营风险。传统风险管理方法难以应对网络风险的动态性和相关性，同时企业在有限预算下如何分配资本以降低风险，成为亟需解决的问题。企业如何科学评估网络风险，并在预算约束下实现**网络安全防御投资**、**网络安全保险**和**风险准备金**的最优配置？传统方法通常无法将这个问题的经济性分析与网络系统的结构性信息有效结合起来，导致决策不够精细。

针对这一问题，清华大学经济管理学院金融系教授冯润桓与其合作者香港大学副教授 Wing Fung Chong、康奈尔大学博士生胡兆轩和俄亥俄州立大学助理教授张临风，在保险与风险管理领域国际顶级期刊 Journal of Risk and Insurance 上发表研究论文“Cyber Risk Assessment for Capital Management”。 研究提出了**“双支柱”框架**，旨在帮助企业在预算约束下，利用网络系统的结构性信息实现网络风险管理的最优策略。

该框架的第一个支柱是基于级联模型（Cascade Model）的网络风险评估。其整合了外在网络威胁、系统漏洞、网络安全控制措施、企业资产及安全事故影响，构建张量化损失模型来量化企业在预算期内的潜在损失。第二支柱是资本管理优化。通过设计整体优化模型来平衡事前投资（风险降低）、保险（风险转移）、准备金（风险保留） 三类资本。该模型采用加权目标函数和帕累托优化，并综合考虑机会成本、预算约束及风险偏好，以实现综合财务影响的最小化。

研究在此框架下对历史上的网络安全事故数据进行了分析。研究表明，在无预算限制的情况下，企业采用投资、保险和准备金的综合策略能够实现财务影响最小化。然而，当预算受限时，虽然直接成本有所下降，但由于准备金不足导致风险暴露，财务影响会急剧上升。此外，安全解决方案价格、保险保费、机会成本以及管理偏好等参数对最优策略具有显著影响。行业层面，小企业因预算紧张通常依赖准备金，而大型企业更倾向于采取多元化策略；同时，风险评估需结合主动扫描，以避免低估潜在攻击路径。

该框架首次将网络系统的结构性信息与精算风险建模融合，提供了科学的资本分配方案，兼顾经济性与安全性。研究为企业制定网络风险管理策略、网络安全保险设计及监管标准提供理论依据，并可扩展至多组织协同管理和动态多期模型。

供稿：科研事务办公室　编辑：杨海琴　责编：吴淑媛 赵霞