

关于加快提升全市中小企业网络信息安全能力的建议

领衔代表：夏斌

一、基本情况

网络信息安全建设是保障企业数字化转型的重要环节。2024年12月，工业和信息化部、财政部、中国人民银行、金融监管总局四部门联合发布《中小企业数字化赋能专项行动方案（2025—2027年）》， “全面增强中小企业数据与网络安全防护能力”作为重点任务之一，进一步聚焦中小企业数据与网络安全。浙江省经济和信息化厅也发布了《关于加强中小企业网络安全管理的指导意见》，旨在夯实网络与信息安全基础，强化网络与信息安全应急处置，并切实做好关键信息基础设施安全防护。宁波市针对企业的安全需求，也已建立了强大的云上态势感知能力与全面的安全架构体系，可提供包括网络攻击监测、攻击溯源、攻击防护等方面的专业安全服务。

但是近年来，黑客攻击方式呈现多样化、复杂化、新型化的趋势，因网络信息安全问题引发的企业数据泄露问题时有发生，企业面临的网络威胁日益增加。网络信息安全保障需要政府、运营商、企业等多方的共同努力。

二、主要问题

目前宁波中小型企业数量众多，全市市场主体达 141 万余户。数字化已经成为中小企业转型升级的必由之路，但随着企业数字化的推进，网络信息安全问题也日益突出。主要体现在以下几点：

（一）企业网络信息安全意识不够。随着产业数字化的进一步升级，面临网络攻击的范围不断扩大。中小企业长期以生产经营为核心，数字化、信息化以生产要素为主，但网络信息安全意识薄弱，安全防范措施不力。例如：2024 年 4 月，宁波北仑某企业的 OA 系统遭受黑客攻击并被篡改涉政有害页面，造成了不良的社会影响。

（二）企业网络信息安全能力薄弱。中小企业受限于资金、技术、人才等客观因素，缺乏足够的网络信息安全能力，如防火墙、入侵检测系统、防毒软件等，但如单独采购安全设备，需要配置相应的网络信息安全管理人才，成本上有一定的压力，因此需要政府侧的引导和扶持。

（三）企业网络信息安全投入意愿不强。由于网络信息安全投入对于中小企业短期来说没有相应的产出，中小企业投入网络信息安全意愿不强，对网络信息安全投入可以长期保护企业免受安全威胁的侵害、维护企业的声誉和客户信任的认识不足。

（四）网络信息安全人才优势没有充分发挥。近年来依托网络安全技能竞赛及各类攻防演练，宁波市已培养了一大批网络

安全人才，但是没有从产业链、生态链上进行统筹和设计，实际效用发挥不足。

三、意见建议

（一）探索设立中小企业网络安全服务机构。建议相关部门适时成立中小企业网络安全服务机构，一方面搭建中小企业网络空间安全服务平台，实现网络态势感知、漏洞常态扫描、威胁情报共享、流程闭环跟踪等，以此提高全市的网络安全应急处置能力；另一方面发挥人才集聚优势，组建专门团队，提供安全风险监测及评估、分析研判及咨询指导等一站式服务，定期开展攻防实战演练、网络安全培训等，提高中小企业对网络信息安全重要性的认识，激发中小企业加大网络信息安全建设投入的积极性。

（二）整合多方力量攻坚中小企业网络安全解决方案。打造网络信息安全产业合作生态圈，以协会或联盟等形式，整合运营商、安全厂商、供应链企业、中小企业代表等力量，共同谋划制定行业标准和规则，在设计、开发、生产数字产品时充分考虑到各种安全隐患，在系统的底层逻辑、底层框架、底层代码中重点体现内生安全需求，从而增强网络安全风险防范能力，实现数字技术、数字产品、数字经济的“普遍安全”。

（三）优化政策补贴降低网络信息安全投入门槛。建议政府加大中小企业网络信息安全引导性补贴，一方面通过中小企业网络安全服务中心提供零成本或低成本、高安全性的普惠服务；另一方面，发挥安全厂商的产品、能力优势和运营商的服

务优势，推动各主体向中小企业提供更低价格的网络安全类产品，或者对购买安全产品与服务的中小企业予以一定比例的补贴。在降低中小企业网络信息安全投入成本的同时，消除受网络攻击、数据泄漏的后顾之忧。

（四）完善“网络安全人才生态链”建设。围绕数字经济新生态、网络安全新范式，加强内部培训与高校联动，促进教育链、人才链、创新链、产业链的深度融合与协同发展。健全以创新能力、质量、实效、贡献为导向的科技人才评价体系，遴选并推广一批产业发展急需的网络信息安全人才培养项目，从人才制度、体系和奖励机制等多方面促进人才建设。

（五）加快网络信息安全学科专业建设。推动高等院校、职业院校加强网络信息安全相关学科专业建设，发挥学科引领和带动作用。在高校相关课程中融入内生安全最新研究成果，鼓励中小企业深度参与内生安全人才培养工作，形成内生安全人才培养、技术创新、产业发展的良性生态。