文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

网络安全应急管理能力提升研究

闫涛
新疆维吾尔自治区人力资源和社会保障厅
DOI:10.32629/acair.v4i3.21346

[摘　要] 本文主要研究怎样提高网络安全应急能力,以解决目前网络安全领域存在的主要问题。结合高校及有关行业网络安全应急管理的实践,从体系建立、技术应用、管理改善、人员培训四个方面进行分析。研究结果表明,健全组织架构和协同机制、加强技术支撑体系、改善应急管理流程、提高人员专业素质,可以明显提高网络安全应急响应速度和处置水平,给各个行业的网络安全应急管理工作提供系统的解决办法,对网络空间安全和数字化健康发展的保障有重要的实践意义。
[关键词] 网络安全；应急管理；能力提升；体系构建；技术支撑
中图分类号：G250.72　**文献标识码**：A

Research on Improving Network Security Emergency Management Capability

Tao Yan
Department of Human Resources and Social Security of Xinjiang Uygur Autonomous Region
[Abstract] This paper mainly studies how to improve the emergency response ability of network security, in order to solve the main problems existing in the field of network security. Combined with the practice of network security emergency management in Colleges and universities and related industries, this paper analyzes from four aspects: system establishment, technology application, management improvement and personnel training. The research results show that improving the organizational structure and coordination mechanism, strengthening the technical support system, improving the emergency management process, and improving the professional quality of personnel can significantly improve the speed of network security emergency response and disposal level, provide systematic solutions for network security emergency management in various industries, and have important practical significance for the protection of Cyberspace Security and the healthy development of digitalization.
[Key words] network security; emergency management; capability improvement; system construction; technical support

引言

在数字经济不断演进的背景之下,互联网已经成为支撑经济社会运转的主要基础设施,在教育、政务、金融等各个领域中起着不可取代的作用。伴随着网络信息技术的普及,恶意程序攻击、数据泄露事件、勒索软件威胁等安全问题不断出现,这些情况既造成巨大的经济损失,又给重要的信息安全带来严重危害,甚至危及到社会的稳定。传统的依靠被动防护的网络安全管理方式已经不能适应复杂的、多变的安全威胁环境了。在此情况下,网络安全综合治理体系中的一项重要组成部分即应急管理体系就具有了特别重要的意义——其效能直接影响安全事件所造成的损害及处理效果的好坏。本文根据当前网络安全应急管理所面临的问题,从实际出发,提出切实可行的改进措施,从而创建出一个系统化、标准化、高效协同的应急反应体系,这是形成现代网络安全治理体系的一种重要途径,也是加强我国信息安全水平的有效方式。

1 网络安全应急管理现状与面临的挑战

1.1网络安全事件演变特征

当前网络安全事件的复杂性与多样性日益凸显,攻击手段不断升级迭代。恶意软件与病毒呈现出隐蔽性强、传播速度快的特点,通过漏洞利用、社会工程学等多种方式渗透入侵,给检测与防御带来极大难度。数据泄露事件集中爆发,敏感信息管理不当、系统漏洞未及时修复等问题成为主要诱因,涉及用户隐私、商业机密等核心数据的泄露事件造成的损失难以估量。

1.2应急管理现存突出问题

应急管理组织架构不完善是当前普遍存在的问题。部分单位未建立常态化的应急管理机构,缺乏明确的职责分工与协同

机制，导致安全事件发生后出现权责不清、推诿扯皮的现象，延误处置时机。监测预警能力不足制约了应急响应的主动性，现有监测系统对异常流量、可疑行为的感知能力较弱，缺乏自动化、智能化的监测工具与分析平台，使得安全事件发现存在滞后性，难以在萌芽阶段有效遏制风险。应急响应流程缺乏标准化规范，未建立科学的事件分级机制，不同级别事件的处置程序、责任主体不明确，跨部门、跨区域协同处置效率低下。资源配置不均衡问题较为突出，专业技术人才短缺、技术设备更新不及时，部分地区和单位因资金、技术等限制，难以满足应急管理的实际需求。人员安全意识与专业技能不足，缺乏常态化的培训与演练机制，导致面对突发安全事件时应对能力薄弱，无法快速有效开展处置工作。

1.3新技术带来的额外挑战

新一代信息技术的快速发展为网络安全应急管理带来新的挑战。5G、物联网、人工智能等技术的广泛应用，使得网络边界不断扩大，设备接入数量激增，网络拓扑结构愈发复杂，安全防护难度大幅提升。人工智能技术被用于编写恶意代码、自动化攻击，攻击手段更加智能高效，传统防御技术难以有效抵御。区块链、云计算等技术的应用，使得数据存储与传输模式发生变革，数据安全保护面临新的风险点。同时，网络安全应急工作的时间窗口不断缩短，漏洞公开后，攻击工具的研发速度往往快于补丁修复速度，给应急处置留下的反应时间极为有限，进一步加剧了应急管理的压力。

2 网络安全应急管理能力提升的核心维度

2.1组织架构与协同机制构建

科学合理的组织架构是提升应急管理能力的基础保障。应建立层级分明、权责清晰的应急管理组织体系，设立校级或单位级网络安全应急管理委员会作为决策机构，由高层领导牵头，统筹规划应急管理工作，制定总体策略与重大决策，协调资源分配。在决策机构之下，组建由信息技术、业务部门、安全专家等组成的技术支持小组，负责日常监测、技术分析、应急处置等具体工作，定期开展安全评估与系统加固。明确各部门网络安全责任岗，配备专职人员负责日常安全管理与事件上报，形成纵向贯通、横向联动的管理链条。建立多部门联合办公模式，通过定期例会、信息共享平台等方式加强沟通协作，打破部门壁垒，实现安全事件处置的无缝对接。同时，加强与外部机构的协同合作，与公安部门、网信办、安全厂商等建立常态化沟通机制，共享威胁情报，在重大安全事件处置中争取外部支持与技术援助。

2.2技术支撑体系优化

技术创新作为提升应急管理能力的核心驱动力，在应急管理的各个关键环节都发挥着举足轻重的作用。

网络安全监测与预警体系当中建立智能化的监控架构有着非常大的战略意义。关键在于把防火墙、入侵检测系统、漏洞扫描工具等众多的安全技术资源整合起来，从而达到对网络环境进行全方位、实时的动态监测的目的。采用融合人工智能算法和大数据分析手段的方法，对日志数据以及流量模式进行深层次的剖析之后，可以对异常情况实施精准的识别并提前预见可能的隐患，从而明显加强预警系统灵敏度和响应速度。应该设计出多层次告警体系，并按照风险级别采用不一样的通知方法（短信或者邮件），这样可以使得核心的信息及时传递给责任人，为应急处理工作赋予有力的支持。

应急处置时科学规划、合理调度各种防护措施的作用是决定性的。利用网络分割装置和入侵检测/防御系统建立纵深防御体系，在遭遇攻击的时候可以迅速封堵威胁的蔓延途径，大大减轻安全事件造成的损失。利用数据加密技术和泄密管控方法来对重要的数据进行保护，防止泄露。建立远程灾备站点，结合虚拟化技术做快速切换的功能，并且定时对重要数据实行多级备份工作，给无法预料到的灾难状况赋予稳定的支援力量，从而保证业务持续运行并且系统可靠。

事后追踪阶段采用攻击溯源技术对网络攻击的产生机制、传播途径及具体执行过程进行分析，给事件调查、责任认定和安全策略改进给予重要的依据和主要的数据支持。

2.3应急管理流程标准化建设

标准化的应急管理流程，乃是提升处置效率的重中之重。要制定完备的应急预案，把应急管理的目标、原则、组织机构以及处置流程等内容清晰明确下来，使其全面涵盖事件检测、报告、分级、处置、恢复、总结等所有环节。

建立科学合理的事件分级标准也颇为关键。依据事件的危害程度、影响范围以及处置难度，将安全事件细分为轻微、一般、重大、特大这四个等级，并且明确不同等级事件的启动条件、处置程序以及责任主体。

应急响应流程同样需要规范。一旦事件发生，要迅速完成事件的核实与等级判定工作，随即启动相应的应急预案，各部门依照职责分工有条不紊地开展处置工作，切实保障处置工作能够有序且高效地推进。

2.4人员素养与队伍建设

应急管理工作的主体是人，人的素质、能力对管理效果起决定性的作用。为了提高人员素质，必须创建起多层次、常态化的培训体系，根据各个岗位人员所承担的工作职责和要求来制订出相应的培训计划。

对普通员工开展网络安全基础知识、安全行为规范等各方面的培训，提高员工的安全意识，降低由人为因素引发的网络安全事件。技术人员需要参加应急处置技能、新型攻击手段应对、安全技术工具使用等各方面的专项培训，提高技术人员的技术操作能力及应急处置能力。面向管理人员开展应急决策、资源协调、团队管理等各方面的培训，提高应急指挥、协调能力。

3 网络安全应急管理能力提升的实践路径

3.1加强顶层设计和制度保障

把网络安全应急管理纳入到单位整体发展战略之中，确定应急管理目标、任务和实施途径，制订中长期发展规划。完善有关的规章制度，细化应急管理的各项要求，明确各个部门、各个岗位的安全职责，保证应急管理工作有法可依、有章可循。建立

完善的考核评价制度，把应急管理工作成效作为部门和人员绩效考核的重要内容，定期开展考核评估，对未履行安全职责、处置不当造成损失的单位和个人进行问责，倒逼责任落实。加强政策扶持和资金投入，加大网络安全应急管理的财政支持力度，用以推进技术设备更新、人才培育、训练演习等工作，从而给应急处置能力改善赋予强有力的支撑。

3.2推动技术融合、创新应用

加快网络安全应急管理领域技术革新与研发步伐，调动企业、科研机构等各类主体的积极性，集中精力推进有关关键共性技术研发工作，促使我国自主拥有应急技术系统。推进新技术同应急管理相融合，依靠大数据技术创建起威胁情报分析平台，把内外部的威胁信息整合起来，从而达成风险精准预估的目的，采用区块链技术保证应急数据的真实性与安全，加强数据共享及追溯的速度，依靠人工智能技术开展应急响应的自动化和智能化工作，加快处置速度并提高准确程度。创建技术交流和分享机制，推进各个地区、各个行业之间技术经验的交流，推广先进的适用技术及解决办法，达成技术资源的共享。

3.3创建多元协同治理结构

网络安全应急管理工作要依靠多方参与、共同治理。政府部门要加大统筹力度，完善网络安全应急管理工作法律法规及政策标准，对网络安全应急管理工作加以指引和监督管理，创建起区域和部门间的协同处置机制，调配应急资源。行业组织要起到桥梁和纽带的作用，制定出行业的规范和自律准则，开展行业内交流活动，推广先进的经验、最佳的实践。企业要落实主体责任，完善自身的应急管理体系建设，提升自身的自主防范和处置能力，并且要积极参加行业间的协同，共享威胁情报和技术资源。高校和科研机构要加大理论研究力度和人才培育工作，给应急管理给予智力支撑和人才支撑。创建政府引导、企业为主导、行业自律、社会参与的多元协同治理体系，一起提高网络安全应急管理的整体水平。

3.4建立完善培训演练和持续改进的机制

形成常态化的培训体系，按照网络安全形势发展以及技术更新速度，不断充实培训内容，采用线上线下的培训方式来保证培训的灵活性和有效性。丰富应急演练的形式和内容，根据实际案例来设计演练场景，增强演练的针对性和实战性，定期开展跨部门、跨区域联合演练，提高协同处置能力。建立演练评估和反馈机制，演练结束之后，组织专家对演练过程和效果进行全方位的评价，找出存在的问题和不足，提出改进意见，及时改进应急预案和演练方案。加强持续改进，依据培训演练成果、安全事件处置经验、技术发展动向等，定时对网络安全应急管理体系展开改良完善，持续加强应急管理能力，顺应不断改变的网络安全局势。

4 结论

网络安全应急管理能力提升属于一项系统工程，牵涉到网络空间安全以及经济社会稳定发展的方方面面。目前网络安全形势日益复杂，应急管理也存在着诸多问题，需从组织架构、技术支撑、流程规范、人员培养等多方面着手进行改善与提升。创建科学合理化的组织架构和协同机制，加强智能化技术支撑体系，制定标准化的应急管理流程，提高人员的专业素质和队伍建设水平，可以有效地提高网络安全应急管理的主动性、针对性和实效性。还要加强顶层设计和制度保障，推进技术融合与创新应用，创建多元化协同治理体系，健全培训演练和持续改进机制，塑造起全方位、多层次的应急管理格局。随着数字化技术的不断发展，网络安全应急管理工作将会遇到越来越多的新问题，必须继续进行研究，不断探索创新，使应急管理能力不断提高，为网络空间安全提供强有力的保障。

[参考文献]

[1]孙培岩.智慧校园高校网络安全应急管理体系研究与实践[J].微型计算机,2025(8):100-102.

[2]王海英.网络安全事件应急管理对策研究——以青海开放大学为例[J].漫科学(科技应用),2025(6):153-155.

[3]孙小丹.人工智能技术在网络安全及数据管理中的应用[J].闽西职业技术学院学报,2023,25(3):111-115.

[4]张杰.信息时代网络安全应急管理策略研析——评《网络安全应急管理与技术实践》[J].科技管理研究,2023,43(15):I0010.

[5]杨海.网络安全应急管理科技支撑体系建设研究[J].电脑知识与技术,2023,19(17):85-88.

作者简介：

闫涛(1984--),男,汉族,新疆乌鲁木齐人,副高级,毕业于武汉科技大学计算机科学与技术专业,现任职于新疆维吾尔自治区人力资源和社会保障厅,担任政策咨询服务中心(社保卡管理中心)高级工程师,研究专业：计算机科学与技术。