网络安全应急响应体系的构建与实践

宣俊
中核第七研究设计院有限公司，山西 太原 030012

DOI: 10.61369/TACS.2026010023

摘　　要： 近些年，随着数字化时代来临，网络已深度融入社会生产生活的各个领域并成为核心基础设施。然而，网络环境日益复杂、多变，这对网络安全保障工作提出了全新要求。在此形势下，企业亟须构建一套科学、高效、可落地的网络安全应急响应体系，既能降低网络安全事件造成的损失，也能强化网络安全风险防控能力，规范网络安全应急处置行为，促使企业快速、有效地应对各类网络安全事件，为企业实现有序运营提供良好的网络环境。对此，本文首先阐述网络安全应急响应体系的构建意义，接着提出来一系列行之有效的构建策略，以期为相关研究者提供一定的参考与借鉴。

关 键 词： 企业；网络安全；应急响应体系；构建

Construction and Practice of a Cybersecurity Emergency Response System

Xuan Jun
China Nuclear No.7 Research and Design Institute Co., Ltd., Taiyuan, Shanxi 030012

Abstract: In recent years, with the advent of the digital era, the internet has been deeply integrated into all fields of social production and life and has become a core infrastructure. However, the network environment has become increasingly complex and volatile, posing new requirements for cybersecurity assurance work. Under this situation, enterprises are in urgent need of building a scientific, efficient, and actionable cybersecurity emergency response system. Such a system can not only reduce the losses caused by cybersecurity incidents, but also strengthen cybersecurity risk prevention and control capabilities, standardize cybersecurity emergency disposal behaviors, and enable enterprises to respond to various cybersecurity incidents quickly and effectively, thereby providing a sound network environment for the orderly operation of enterprises. In this regard, this paper first elaborates on the significance of constructing a cybersecurity emergency response system, and then puts forward a series of effective construction strategies, aiming to provide certain references for relevant researchers.

Keywords: enterprises; cybersecurity; emergency response system; construction

一、网络安全应急响应体系的构建意义

（一）有利于降低网络安全事件造成的损失

在网络安全事件发生后，企业损失与其能否有效且快速地进行应急处置息息相关。完善的网络安全应急响应体系，不仅能够预先制定详细而全面的应急响应流程，明确各部门、工作人员的职责分工，也能构建密切配合、高效的协同机制，面对网络安全事件时，企业迅速地启动事先精心准备好的应急处置预案，并对网络安全应急响应工作进行深入研判，精准地分析事件的起因、性质、危害程度等，根据分析结果采取针对性遏制措施，阻止安全事件进一步恶化或蔓延[1]。此外，网络安全应急响应体系能够全面核对直接损失与间接损失，为后续的保险理赔、责任认定及改进措施制定提供依据。这样，可以最大限度地减少因网络安全事件所导致的各种损失，以最快的速度让整个组织的运营重回正轨[2]。

（二）有利于强化网络安全风险防控能力

网络安全应急响应体系通过建立常态化的风险监测机制，能够对网络系统中的潜在威胁进行实时扫描与动态分析，及时识别出系统漏洞、恶意代码传播、异常访问行为等风险隐患。在风险尚未演变为实际安全事件前，体系可依据预设的风险评估模型，对风险等级、影响范围及可能造成的后果进行精准研判，为企业或组织提供科学的风险预警[3]。同时，基于风险评估结果，应急响应体系能够指导相关部门制定针对性的风险处置预案，如对高危漏洞进行优先修补、对重点业务系统采取强化防护措施等，从而将风险控制在可控范围内，避免风险累积引发严重安全事件。此外，通过对应急响应过程中积累的风险数据进行复盘与分析，还能不断优化风险防控策略，提升对新型网络安全威胁的预判能力和应对水平，形成“监测－预警－处置－优化”的风险防控闭环[4]。

（三）有利于规范网络安全应急处置行为

在面对安全事件时，网络安全部门往往需要多方参与才能解决，如果缺乏统一的标准规范，会出现推诿扯皮、处置程序混乱、处置手段任意等问题，影响应急处置效果甚至造成新的风险点。完善的网络安全应急响应体系可通过标准化处置流程及操作规范，明确各主体参与的职责分工、工作流程和协作方式[5]。如在事故发现阶段，可以提供不同监测手段精准定位问题，明确上报路线图、时限标准和要求；在分析研判阶段，制定统一的事故等级判定标准以及分析研判方法，对事态性质、影响范围及危害程度作出准确判断。除此之外，应急响应体系中还规定了在处置过程中的发布信息、内外部沟通、档案留存等内容，以确保处置有章可循、有据可依，避免因不当行为或执行不到位导致事态升级，进而提升处置工作规范化程度以及严谨性水平，保障网络安全应急响应工作得以高效、有序地开展[6]。

二、网络安全应急响应体系的构建策略

（一）明确责任主体，强化统筹协调

在网络安全应急响应体系构建中，明确责任主体是重要环节，应明确各职能部门及人员在网络安全应急响应中所承担的具体职责及权限。通常情况下，企业应当成立由负责人牵头的网络信息安全应急处置工作领导小组，全面负责应急决策、指挥调度等工作，确保应急响应工作的有效性、高效性[7]。另外，企业成立专门的应急响应执行小组负责具体工作，如安全人员、系统管理人员以及业务人员等分别开展监测、研判、处置、恢复重建等工作。同时，企业也要明确各个职责部门在应急管理中的具体作用，如快速上报安全隐患情况、业务情报支持、协助系统整改等等，形成“一头主责、层层担责、联动配合”的责任体系。此外，企业应当构建常态化沟通协商机制，如经常性的应急响应工作组会议制度、建立跨部门信息共享机制等，强化各相关部门之间的信息交换以及协作配合，确保快速有效地对网络安全危机作出反应并妥善处置，避免因推诿扯皮而贻误时机，从组织保障层面为网络安全应急响应工作有序控制奠定坚实基础[8]。

（二）规范处置环节，提升响应效率

为了保障处置的有效性与精准性，既要做好规范化建设又要做好技术支持。对此，企业应当制定“监测预警－研判决策－应急处置－恢复常态－总结提升”的标准化作业流程，明确每个流程的触发条件、工作内容、责任人及完成时间。例如，在预警阶段采用入侵检测仪、日志分析仪等对网络流量信息、系统日志、用户行为等进行实时采集，并设定一系列的警示阈值，当出现异常事件的时候及时产生报警；在决策判断阶段制定相应的判断标准，如潜在风险、危机程度、风险类型等，快速判断事件等级及处置优先级，确保后续做到精准施策[9]。另外，在应急处置方面，企业要制定分级处置方案，根据不同级别的危机采用相应的技术手段，比如，面对勒索病毒，立即隔离受感染主机，切断病毒传播路径，并启用备份文件等措施。在系统恢复阶段，企业要贯彻“最小损伤”的原则，在主服务系统恢复后，通过数据校对、缺陷修补等形式保证系统再次运行后的安全性；在后期复盘环节，生成全面的突发事件报告，并总结处理经验，完善预防及防御措施[10]。除此之外，企业通过自动化应急响应系统，有机整合威胁情报库、漏洞扫描工具、自动化补丁修复等各类资源整合，实现从告警信息到具体执行的半自动化甚至全自动执行，在很大程度上节省了响应时间，能够快速进行数据恢复和服务重启，从而极大地提升整体的应急响应效率[11]。

（三）夯实保障基础，确保处置有力

保障基础的夯实是应急响应体系有效运转的前提，需从多维度入手构建坚实支撑。在队伍建设方面，应组建专业化的应急响应团队，团队成员需涵盖网络安全、系统运维、数据恢复等多个领域的技术人才，定期开展实战化演练和技能培训，提升团队成员对复杂网络安全事件的分析研判能力、应急处置能力和协同作战能力，确保在突发事件发生时能够迅速集结、高效应对[12]。资源保障上，要加大对网络安全应急响应的资金投入，配备先进的应急响应工具、设备和专业软件，建立应急物资储备库，确保应急处置过程中所需的硬件设备、软件工具、数据备份介质等资源充足且状态良好。同时，加强与网络安全服务机构、科研院所等外部力量的合作，建立应急支援机制，形成内外联动的资源保障网络，为应急处置提供技术支持和资源补充。此外，还需完善应急响应相关的制度规范，明确应急响应过程中的责任分工、工作流程、资源调配、信息报告等要求，确保应急处置工作有章可循、规范有序，为应急响应的有力实施提供全面保障[13]。

（四）强化技术支撑，提升处置效能

在网络安全应急响应体系中，企业也不断强化技术支撑基础，通过充分应用网络信息安全监测预警技术，建设具备在线监测、智能研判以及异常识别功能的信息安全感知平台，综合采集、多维分析网络通信、日志行为、用户活动等关键指标，形成覆盖全网的信息安全态势感知体系，实现早期预警、精准定位、及时报警的目标[14]。此外，企业还应当积极引入人工智能、大数据技术等新型技术，强化网络安全危机的自动化判定、智能化决策水平，例如，企业依托机器学习算法结合历史安全危机案例进行模拟训练，搭建智能化攻击检测模型，能够快速区分正常网络行为和恶意攻击行为，缩短网络安全危机判定时间。同时，加强应急响应技术体系建设，在集成漏洞检测、入侵监测、信息恢复、攻击追踪等功能模块基础上，建立综合、高效的应急处置技术支持系统，实现网络安全危机在发现、分析、阻断、清除和恢复过程中的全封闭式流程化管理。在这个过程中，企业应当制定统一的技术规范及标准，确保各类新型技术之间实现信息共享、相互配合，避免出现信息壁垒现象，提升应急处置整体的技术水平[15]。

三、结语

总而言之，网络安全应急响应体系的构建是一项系统工程，它不仅是企业应对网络安全威胁的关键屏障，也是保障业务连续性的重要举措。对此，企业可以从明确责任主体，强化统筹协

调；规范处置环节，提升响应效率；夯实保障基础，确保处置有力以及强化技术支撑，提升处置效能等策略着手。这样，将不断提升应急响应的科学性、精准性和时效性，促使企业有效应对各类网络安全挑战，为数字化转型和业务健康发展保驾护航。未来，随着人工智能、大数据等新兴技术在网络安全领域的深入应用，网络安全应急响应体系也将朝着更加智能化、自动化和协同化的方向发展，为构建更稳固的网络安全防线提供持续动力。

参考文献

[1] 简金海 . 山地风电场网络安全预警与应急响应体系 [J]. 网络安全和信息化 ,2024,(11):46-48.
[2] 陆明典 . 气象业务网络安全应急响应体系研究 [J]. 网络安全和信息化 ,2024,(06):135-137.
[3] 蒋帆 . 网络安全事件响应与应急处理流程探讨 [J]. 通讯世界 ,2024,31(01):46-48.
[4] 麦欢怡 . 电信运营商网络安全应急响应体系设计与应用 [J]. 电信快报 ,2023,(08):25-30.
[5] 盘采华 , 杨馨蕾 , 王雨倩 . 科研院所网络安全应急响应体系模型设计 [J]. 网络安全和信息化 ,2023,(08):111-114.
[6] 肖伟 . 网络安全应急响应管理平台的设计与实现 [J]. 信息记录材料 ,2022,23(09):68-71.
[7] 束维国 . 基于安全编排自动化与响应技术在网络安全应急响应中的应用探索 [J]. 现代工业经济和信息化 ,2022,12(08):112-114.
[8] 徐文君 . 以态势感知为中心的网络安全应急响应工作体系研究 [J]. 电子技术与软件工程 ,2022,(12):9-12.
[9] 刘晨晖 , 王能民 . 基于压电式理论的网络安全事件应急响应体系：美国的实践启示 [J]. 情报杂志 ,2021,40(03):112-117+31.
[10] 吕世军 , 余杨 . 打击治理电信网络新型违法犯罪纳入安全应急响应体系的设想 [J]. 信息网络安全 ,2020,(S1):67-70.
[11] 黄道丽 , 原浩 . 我国关键信息基础设施网络安全应急响应的法律保障 [J]. 中国信息安全 ,2020,(03):42-43.
[12] 罗伟 . 浅析网络安全新形势下如何完善提升应急响应机制 [J]. 中国信息安全 ,2020,(03):50-52.
[13] 徐原 . 国际网络安全应急响应体系介绍 [J]. 中国信息安全 ,2020,(03):32-35.
[14] 张永印 . 网络安全应急响应的创新与实践 [J]. 中国信息安全 ,2020,(03):44-46.
[15] 谢瑞璇 . 建立有效及时的网络安全应急响应体系 [J]. 中国信息安全 ,2020,(03):47-49.

