**中国银行网络安全体系建设思考与实践**

中国银行数据中心总经理 李世京

目录

[**中国银行网络安全体系建设思考与实践** 1](#_Toc519453856)

[**加强顶层设计，完善信息安全治理机制** 1](#_Toc519453857)

[**覆盖全生命周期，深化系统安全漏洞管理** 2](#_Toc519453858)

[**打造SOC，强化一体化网络安全威胁管理** 2](#_Toc519453859)

[**推进智能化网络金融事中风控能力** 3](#_Toc519453860)

[**聚焦前瞻性研究，加快专业人才培养** 3](#_Toc519453861)

[**未来努力方向** 4](#_Toc519453862)

面对日益严峻的威胁和挑战，中国银行持续完善科技风险治理机制，将网络安全风险作为集团重要风险进行统一管控。在技术防御体系方面，提出了“建立以主动防御为方法，纵深防御为基础的一体化网络安全防御体系”的目标，从一体化安全技术架构、常态化安全漏洞管理、主动化安全威胁管理、智能化业务风险防控、专业化安全队伍建设等五大领域重点发力，突破传统离散、被动的防御模式，提升信息系统健壮性，强化主动应对网络攻击的能力。

**加强顶层设计，完善信息安全治理机制**

中行持续完善信息安全管理策略、制度规范和技术标准，将信息科技风险纳入全行风险管理三道防线统一管控；按照信息安全专业领域细化安全管理组织架构和职责分工，形成自上而下，垂直贯穿海内外各级机构的信息安全管控体系；以整体防御框架及安全标准规范为依托，从企业级的视角, 将安全管控机制嵌入到需求开发、安全测试、投产准入、运维加固的全生命周期之中；健全管理机制，在总行的统筹规划下，形成研发与运维、业务与科技、总行与分行之间紧密协同、守土有责的管理模式，做到任务层层分解、措施执行有力、考核落实到位、责任落实到人.

健全全行信息安全组织架构和岗位配置，明确了信息安全管理对象和管控要求，通过ISO27001、ISO20000等国际标准认证，统一了全行信息安全管理的标准和方法，建立了安全管理机制和流程，提升了IT风险的管理水平。同时，将监管要求与国际标准相结合，梳理23个国家和地区的法规与监管要求，对标国内外网络安全最佳实践和技术规范，设计了涵盖7个领域26个子域69个子目标的内控框架，全面提升监管遵从与合规运营能力。

**遵循最佳实践，推进网络安全技术架构建设**

完善的技术框架是整个防御体系建设的先决条件和重要指导。中国银行深入分析面临的安全威胁，建立了9大分类的41项网络安全威胁模型，对标ISO 27001、PCI-DSS、《信息系统安全等级保护》等国内外网络安全最佳实践和技术规范，同时借鉴P2DR、PDRR、《自适应安全框架（ASA）》等主流网络安全框架，实现网络安全建设遵从法规、符合标准、接轨业界技术发展新要求。

根据整体信息安全管理框架，从空间和时间维度不断整合优化传统防御技术，形成了统一管理、梯次部署、纵深防御的网络安全防御技术框架。对外，严格实行内外网隔离，通过云端、运营商和本地三重DDos防御、入侵检测等技术，能够识别与防护3~7层网络攻击；对内，通过网络分区隔离、全行域用户管理及接入控制，以及防病毒、防篡改、防泄密等技术实现了常见安全威胁的防范和数据安全的保护。通过安全设备策略整合、威胁事件关联分析，以及高等级威胁监测等技术，具备了对于APT、精准式网络攻击的分析识别能力。

**覆盖全生命周期，深化系统安全漏洞管理**

近年来，中国银行持续加大对应用安全管控的投入，围绕可用性和安全性，完善非功能技术标准，建立了覆盖全生命周期应用系统安全管理机制，针对各类安全风险场景制定差异化应对策略，提升产品自身安全性。

一是建立全生命周期的漏洞管理机制。在设计阶段，明确安全要求、提前采取安全措施；在开发阶段，建立代码扫描和安全测试机制，降低应用漏洞风险；在投产运维阶段，进行上线前准入安全测试，定期进行漏洞扫描和渗透性测试，及时发现安全隐患并积极整改。

二是建立多维度、立体化漏洞评测机制。自主研发了安全漏洞风险计量标准及工具平台，建立了覆盖总、分行的安全漏洞扫描系统，定期自主开展漏洞扫描及远程渗透测试工作。聘请第三方专业机构定期开展互联网应用系统独立安全评估，发现问题及时进行整改。此外，结合网络安全情报，跟踪互联网漏洞信息及业内网络安全风险事件，向全辖发出风险提示，并及时处置。

目前，中国银行已形成安全漏洞发现、验证和修复的跨机构跨部门协同联动工作机制，有效提升了系统安全能力。

**打造SOC，强化一体化网络安全威胁管理**

中国银行持续强化安全威胁监测技术，全力打造7\*24小时不间断安全运营中心SOC。集中收集各类日志信息，并结合网络流量数据进行关联分析，实现了威胁监测的一体化集中管理。通过引入威胁情报、大数据分析等新兴技术，强化了对于高级持续性威胁（APT）和精准式网络攻击的实时发现及智能化预警能力。

在SOC建设过程中，配套建立了安全威胁运维机制，形成了监控、预警、处置、调查、加固的威胁运维管理流程，实现威胁监测、应急等各项工作标准化。目前，日均自动化监控日志超过3.7亿条，网络流量数据超过4.9亿条。截至2017年10月底，识别和拦截外部网络安全威胁事件万余起。阻断来自75个国家和地区的外部攻击地址3808个，成功防范了拒绝服务、网络入侵、网页篡改、信息泄露等大规模网络攻击,有效保障了我行金融业务的发展。

**推进智能化网络金融事中风控能力**

近年来随着跨境服务、跨业合作、跨界经营，以及新技术应用和新商业模式的出现，银行风控方法发生重大变化。中国银行以事中监控为核心，以线上渠道和网络金融业务为服务目标，综合运用大数据、云计算、人工智能等先进技术，构建了主动实时、高效智能的网络金融业务风险管控平台。

通过业务风控能力建设，中国银行事中业务风险管控实现了风险能力价值共享，运营能力专业集中。在控制风险的同时，识别和抵御网络金融欺诈，全面保障了个人网银、个人手机银行和中银E贷等主要网络金融渠道和产品的交易安全，进一步提升了我行网络金融风险交易监测能力。

**聚焦前瞻性研究，加快专业人才培养**

我行积极开展自主可控网络安全技术前瞻性研究和运用。2016年，我行与专业安全机构及知名高校联合建立了“金融信息安全联合实验室”，着力加强“安全新技术”及“新技术安全”领域的研究运用，目前已在安全威胁态势感知模型、量子通讯加密技术、总分机构互联标准设计、商业化波分复用技术研发等方面取得了积极进展。

为加强网络安全人才培养，中国银行专门成立了信息安全专业技术团队，负责全行网络攻防工作，在实战中不断锤炼提升队伍专业化能力。每年定期进行防DDos攻击、防病毒、精准式网络攻击、社会工程攻击实战演练。今年开展的钓鱼邮件社会工程实战演练是近年来规模最大的一次实战演练，发送钓鱼演练邮件近万封，覆盖总行管理层及海内外分行各级员工，对于提升全行员工网络安全意识发挥了积极作用，取得了明显的成效。

**未来努力方向**

作为全球系统性重要银行，中国银行的网络安全体系应具备统一指挥、随时应对全球7×24小时安全威胁的监测和应急响应能力，全面、智能、可视化的信息安全威胁态势分析能力，贯穿信息系统生命周期各环节的安全漏洞自动化发现能力。面向未来，中国银行将依据顶层规划，跟踪前沿技术发展，探索建立基于大数据和人工智能技术的主动式安全态势感知模型，进一步提升智能化风控能力，完成云平台等新技术平台安全防御体系的设计、研发和部署，大力加强新型网络安全技术队伍培养，实现对网络安全风险预警、实时监控、关联分析与快速处置的全流程管控。