 DOI: https://doi.org/10.12349/iser.v7i9.11752

Research on the Causes of Cybersecurity Risks and Long-Term Protection Mechanisms in the Context of the Digital Age

Houwei Yu

Southwest Copper Branch of Yunnan Copper Industry Co., Ltd., Kunming, Yunnan, 650101, China

Abstract

In today's context, digital technologies have been extensively integrated into various sectors including government administration, finance, education, healthcare, and business operations, transforming cyberspace into a critical platform for business operations and public services. Advances in cloud computing, the Internet of Things, artificial intelligence, and mobile devices have not only expanded the scope of data utilization but also increased the number of attack vectors and accelerated risk propagation. Current cybersecurity challenges stem from both systemic vulnerabilities, centralized data storage, and supply chain dependencies, as well as ambiguous accountability frameworks, insufficient funding, and inadequate staff awareness of security measures. To establish sustainable protection mechanisms, it is essential to move beyond relying solely on isolated devices or post-incident responses, instead integrating risk assessment, technical defenses, regulatory frameworks, personnel training, and emergency response into a unified approach to enhance the continuous security operation and governance capabilities of network systems.

Keywords

digital era; cybersecurity; risk factors; data governance; long-term protection

数字时代背景下网络安全风险诱因及长效防护机制研究

喻后伟

云南铜业股份有限公司西南铜业分公司，中国 · 云南 昆明 650101

摘　要

在如今的形势下数字技术已经广泛地融入到政务、金融、教育、医疗、企业经营等诸多领域之中，使得网络空间逐渐演变成业务运行、公共服务非常重要的承载平台。云计算、物联网、人工智能还有移动终端这些技术领域的发展不仅拓展了数据利用的边界范围，与此同时还增大了攻击入口的数量并且加快了风险传播的速度。现阶段所面临的网络安全问题一方面是源自系统漏洞、数据集中、供应链依赖等因素，另一方面也和责任界定模糊、投入资金不足、人员防范意识比较薄弱等方面存在关联。若想建立起长效的防护机制，那就应当改变以往单纯依赖单点设备、事后处置的方式，而是要把风险评估、技术防御、制度约束、人员教育、应急响应等内容纳入到一个统一的模式当中，以此来提高网络系统持续安全运行、治理的能力。

关键词

数字时代；网络安全；风险诱因；数据治理；长效防护

1 引言

数字化转型提高信息处理的效率，同时也对传统安全边界产生了改变。业务系统开始从封闭的内网逐步朝着云端部署、跨平台协同的方向转变，员工能够借助移动设备远程访问数据，企业还需和供应商、合作平台、外部服务机构进行信息交换。网络环境的开放性致使风险不再局限于病毒感染、设备故障，而是呈现出身份冒用、数据泄露、勒索攻击、供应链渗透、算法滥用等多种不同的形态。部分单位依旧把网络安全视作技术部门的单独职责，重视设备采购却轻视制度执行，重视故障修复却轻视风险预防，难以应对持续变化的威胁。研究风险形成的机理并建立长效防护机制，是保障数字业务稳定运行、维护数据权益的重要基础。

2 数字时代网络安全风险的基本特征

2.1 风险入口呈现多元化特征

在传统网络系统当中，其访问入口呈现出相对集中的趋势，安全管理工作主要是围绕着机房、服务器、内部终端来展开的。进入数字时代，业务系统连接了云平台、移动终端、物联网设备还有第三方接口，如此一来，攻击者能够从账号口令、应用程序、智能设备、无线网络或者外包系统等

【作者简介】喻后伟（1975–），男，中国重庆人，硕士，高级工程师，从事计算机应用、网络及网络安全等研究。

多个不同位置实施渗透行为。一旦某一低安全等级的设备被成功攻破，那么风险就有可能顺着网络连接进入到核心业务区域当中。远程办公、移动应用的出现，也使得人员访问地点变得更加分散，以往那种凭借单位内外网络来划分安全边界的方式，正逐渐失去作用 [1]。网络安全管理必须要从单一边界防护转变为身份、设备、应用、数据、行为的综合控制，针对每个连接请求展开持续验证。

2.2 安全风险具有快速传导性

数字业务彼此间有着紧密的数据、系统联系，某一个环节要是出现故障，极有可能较快地对多个部门、合作主体造成影响。比如说，身份认证平台遭到攻击之后，多个业务系统有可能会同时无法登录，供应链平台的数据要是出现异常情况，采购、生产、结算、客户服务也可能会受到影响。网络攻击常常会借助自动化工具对漏洞展开批量扫描，能够在较短的时间内使影响范围得以扩大。数据进行集中存储进一步提高风险带来的后果，一旦核心数据库发生泄露，损失不但涉及单条信息，还可能致使商业秘密被暴露，客户权益遭受损害，社会信任度降低。风险传导的速度变快，这就需要单位提高实时监测、快速隔离的能力。

2.3 网络威胁具有较强隐蔽性

有些网络攻击不会马上导致系统瘫痪，而是长时间潜伏来收集账号信息、业务流程、数据结构信息。攻击者可能会利用合法凭证登录系统，从而让异常行为和正常操作混在一起，传统那种依靠病毒特征、固定规则的检测方法很难及时识别出来。内部人员由于误操作、越权访问或者利益驱使造成的数据泄露，同样具有很强的隐蔽性。人工智能生成的钓鱼邮件、虚假语音、仿冒页面使得欺骗性进一步提高，普通用户很难凭借外观判断真假。网络安全防护要留意访问行为、数据流向、操作模式的异常变化，不可以仅仅依靠事后的日志排查。

3 数字时代网络安全风险的主要诱因

3.1 技术架构复杂与漏洞治理滞后

数字化系统一般是由自建平台、云服务、开源组件、第三方应用共同组建而成的，其技术版本众多，接口关系繁杂。有些单位在追求业务上线速度之际，没有同步进行安全测试，导致系统出现了弱口令、接口越权、补丁缺失、配置错误等一系列问题。老旧设备由于兼容性的限制长时间没有更新，这也有可能成为攻击的入口。在软件开发过程当中，如果缺少安全编码、代码审查，那么漏洞就会随着系统投入使用而进入生产环境。

3.2 数据集中利用与权限管理失衡

数据已然成为数字业务颇为关键的资源，单位常常借助集中平台来汇集客户信息、交易记录、运行数据，以此支撑分析决策。然而，数据集中这一情况也使得攻击价值有所提高。部分系统存在权限设置过于宽泛、共用账号、离职人员账户未注销、敏感数据以明文形式存储等一系列问题。业务人员为了提高工作效率，有可能把数据下载至个人终端，或者通过非正式渠道进行传输，进而造成控制链条中断 [2]。第三方机构参与系统运维、数据分析工作时，如果合同责任与访问范围未能清晰界定，同样会致使泄露风险扩大。数据利用与安全保护之间缺乏平衡，这是网络风险持续增多的一个重要缘由。

3.3 管理责任与人员意识存在薄弱环节

网络安全涉及到管理层、技术部门、业务部门、普通用户等多个方面，然而部分单位却把责任过度集中于信息技术人员。业务部门在进行采购系统、开放接口或者使用数据操作的时候，缺乏安全评估环节，一旦出现问题，又很难清晰地界定责任归属。安全制度所涵盖的内容比较笼统，没办法转化为像账号管理、数据传输、设备使用等方面的具体要求。针对人员的培训大多只是停留在观看视频、签署承诺书这种形式上，缺少针对钓鱼邮件、社交工程、移动办公等方面的实际操作演练。员工受方便性因素的驱使，使用简单口令、共享账号或者连接不可信网络，使得技术防护因人为操作而被削弱。管理与人员方面的因素常常是风险形成的重要放大因素。

4 数字时代网络安全长效防护机制的构建路径

4.1 建立分层纵深的技术防护体系

网络安全技术模式要涉及终端、网络、应用、身份、数据等多个方面。单位应当对服务器、终端、云资源、外部接口加以梳理，以此形成动态资产清单，并且依据业务的重要程度来划分安全区域。身份认证能够采用多因素验证、最小权限、持续授权机制，降低账号被盗之后的影响范围。核心数据应当施行分类分级、加密存储、传输保护、备份恢复措施，关键操作要保留完整日志。终端检测、流量分析、异常行为监测能够相互联动，针对可疑活动及时进行告警、隔离、处置。

4.2 完善全生命周期风险管理制度

网络安全管理需要贯穿于系统规划、开发、采购、上线、运行、退出的整个过程。对于新建系统而言，在立项阶段要进行安全需求分析工作，在开发过程当中要实施代码审查、漏洞测试，上线之前要完成权限、配置、应急方案的验证。在运行阶段，应当定期进行风险评估、补丁更新、账号清理工作，对于重要系统要实行变更审批。在采购云服务、外包运维、第三方软件时，要审查供应商的安全能力，并且在合同里面明确数据使用、漏洞修复、事故责任 [3]。当系统停用之后，还需要妥善处理数据迁移、设备销毁、账号注销事宜，防止遗留信息成为新的风险源。

4.3 强化安全教育与岗位责任落实

人员具备安全意识需要通过持续不断的教育、对行为的管理来一步步培育而成。管理层要担负起网络安全方面的

领导职责，把安全要求融入到业务决策、绩效评价当中。技术部门负责进行风险监测工作、进行防护措施的实施，业务部门对系统需求、数据使用还有权限申请承担直接责任，普通员工则要遵守终端、账号、信息传输的相关规范。培训内容应当依据岗位的不同特点来设置，财务人员着重去识别虚假付款指令，管理人员关注敏感信息的保护，运维人员加强高权限账号的管理。

5 网络安全长效防护机制的运行保障

5.1 构建常态化监测与预警机制

网络威胁呈现出持续演化、隐蔽渗透、快速扩散等特性，安全管理不能够仅仅依赖于阶段性检查或者事故发生之后的被动处置方式。单位需要建立一个涵盖网络流量、终端运行、账号登录、数据访问、接口调用情况的常态化监测模式，并且依据正常的业务状态来形成动态基线。对于那些异地登录、短时间内进行批量下载、权限出现异常提高、频繁访问敏感数据、接口调用突然增加等行为，应当按照风险程度来设置分级预警，明确地给出提示、核查、阻断、上报的条件。预警规则还需要结合业务的变化情况持续进行调整，防止因为告警数量过多而使得处置人员出现判断疲劳。安全管理部门应当定期对攻击来源、事件类型、受影响资产、处置结果进行分析，识别系统当中的高频风险、薄弱环节，并且依据这些情况来优化检测模型、访问策略、防护重点。

5.2 完善应急响应与业务恢复体系

网络安全事件一旦发生，能不能快速地控制住风险的传播并且让关键业务得以恢复，这直接关乎到损失的范围、组织运行的稳定性。单位需要针对勒索攻击、数据泄露、账号失陷、系统中断、供应链故障等这些典型的情形来制定专项预案，要明确事件分级、报告程序、技术处置、管理决策、外部沟通等方面的要求。对于核心系统与重要数据，应当建立起本地备份、异地备份、容灾切换的机制，并且要定期去进行恢复测试，从而防止备份文件出现损坏、缺失或者无法使用这类情况。应急演练要设置一些和实际业务贴近的场景，像服务器失联、敏感数据异常外传、高权限账号被盗等，以此检验技术、业务、法务、管理部门的协同效率 [4]。在事件处置完毕之后，要对攻击路径、控制缺陷、响应时效、恢复过程进行复盘，及时修复漏洞、调整权限并将预案完善。这样就能形成发现、隔离、处置、恢复、改进相互衔接的应急闭环。

5.3 建立评价改进与协同治理机制

网络安全的长效防护需要靠持续评价来找出制度执行、技术运行当中的不足之处。单位能够结合业务的特点来设定一系列指标，像漏洞修复及时率、异常告警处置率、高风险账号清理率、备份恢复成功率、安全培训覆盖率等，以此对防护成效做量化分析。内部审计部门和风险管理部门应该定期去检查权限配置、数据使用、系统变更、外包运维等情况，针对重大隐患展开专项审查，避免安全制度仅仅停留在文件方面。评价结果要和责任考核、技术改造、资源投入相联系，让发现的问题能够转变成具体的整改任务。网络攻击常常会跨越组织边界，单个单位很难独立掌握所有风险信息，所以还需要加强跟监管部门、行业机构、技术服务商、供应链伙伴之间的信息共享，及时获取漏洞通报、攻击特征、威胁情报。通过统一接口要求、事件报告规则、应急协作流程，可以提高跨主体风险联防、产业链整体恢复的能力。

6 结语

在数字时代，网络安全风险是由技术漏洞、数据集中、组织管理、人员行为共同作用而形成的，具备入口众多、传播速度快、隐蔽性较强等特性。仅仅依靠防火墙、杀毒软件或者阶段性检查，是很难应对持续变化的威胁的。单位需要建立分层纵深的技术模式，把安全要求融入系统的全生命周期，并且通过岗位责任、人员教育、供应链管理来强化制度的执行。常态监测、应急恢复、审计评价、跨主体协同同样是长效防护不可或缺的环节。网络安全并不是一次性建设任务，而是随着数字业务变化不断进行调整的治理过程 [5]。只有将技术防护、管理约束、人的安全行为有机结合起来，才能够提高风险识别与恢复能力，从而为数字化发展提供稳定可靠的安全环境。

参考文献

[1] 罗巧云.省级应急广播平台网络安全风险与防护策略[J].广播电视信息,2026,33(6)83-86.

[2] 张凡凡.大数据背景下计算机网络安全风险分析与防范策略研究[J].中国宽带,2026,22(5)89-91.

[3] 陈雯.移动互联网时代学生网络安全风险及综合治理研究[J].通讯世界,2025,32(12)39-41.

[4] 沈萍.面向攻击面收敛的网络安全风险治理研究[J].网络安全与数据治理,2026,45(3)17-23.

[5] 张晶,司明星.机房网络安全风险的应对措施分析[J].电子技术,2026,55(2)598-599.