

实验室数智化转型中网络信息安全的重要性探析

杨宇 韩祎陟 韩晶 钱仪嘉

中国海关科学技术研究中心 呼和浩特海关技术中心

DOI:10.32629/jsse.v4i1.19098

[摘要] 随着数字化、智能化技术的发展,数智化转型已成为提升实验室科研效率、数据处理能力与管理水平的重要路径。转型过程中,实验室数据信息面临数据泄露、网络攻击、系统漏洞等多重安全风险,网络信息安全成为制约转型成效的关键因素。本文通过探讨网络信息安全在实验室数智化转型中的重要地位,分析其对实验室数据安全、业务连续性、科研竞争力的影响,提出完善实验室信息安全管理、提升实验室人员意识、制定应急响应计划、升级与优化软硬件设施、与外部安全服务商合作等保障策略,帮助实验室在数智化转型中筑牢网络信息安全“生命线”。

[关键词] 网络信息安全; 数智化转型; 实验室管理; 数据安全

中图分类号: C931.6 文献标识码: A

An Analysis of the Importance of Cybersecurity in the Digital and Intelligent Transformation of Laboratories

Yu Yang Huizhi Han Jing Han Yijia Qian

Science and Technology Research Center of China Customs Technical Center of Hohhot Customs

[Abstract] With the development of digital and intelligent technologies, digital and intelligent transformation has become an important path to improve laboratories' scientific research efficiency, data processing capabilities and management levels. During the transformation process, laboratory data and information are exposed to multiple security risks such as data leakage, cyber attacks and system vulnerabilities, making cybersecurity a key factor restricting the effectiveness of the transformation. By exploring the important position of cybersecurity in the digital and intelligent transformation of laboratories, this paper analyzes its impacts on laboratory data security, business continuity and scientific research competitiveness, and proposes safeguard strategies including improving laboratory information security management systems, enhancing laboratory personnel's awareness, formulating emergency response plans, upgrading and optimizing software and hardware facilities, and cooperating with external security service providers. These strategies are designed to help laboratories fortify the "lifeline" of cybersecurity in the process of digital and intelligent transformation.

[Key words] Cybersecurity; Digital and Intelligent Transformation; Laboratory Management; Data Security

引言

在新一代信息技术与科研创新深度融合的浪潮下,实验室作为科技创新的重要阵地,正加速摆脱传统人工操作、孤立运行的模式,逐渐向数据驱动、智能协同的数智化方向转型。从实验样本的自动化采集、数据的智能化分析,到跨机构科研协作的数字化合作、仪器设备的远程精准管控,数智化技术不仅大幅提升了科研工作的效率与精度,更拓展了实验室的研究边界与空间。

数智化转型带来的“万物互联”格局,让海量精密智能仪器、复杂业务管理系统全面接入网络,形成了多终端、多链路、多数据节点的复杂网络生态。传统“单点防护”的安全模式已难以

抵御针对性网络攻击、数据窃取、设备恶意操控等新型风险,小则导致实验数据失真、仪器运行故障,大则引发知识产权泄露、科研项目中断,直接影响到数智化转型的成效与可持续性。基于此现状,本文聚焦实验室数智化转型的现状与安全需求,深入剖析网络信息安全的重要性,为完善科学有效的安全管理制度提供思路,助力数智化转型平稳、高效落地。

1 实验室网络信息安全风险现状分析

1.1 外部攻击针对性强

随着科研机构数智化转型的持续深入、高价值科研成果的战略意义与经济价值日益凸显,外部攻击者对科研机构敏感数据的关注度显著上升,攻击行为的精准化、靶向化特征愈发突

出。这类攻击不再是无差别的试探,而是对科研机构组织架构、隐私信息、核心研发方向的精准研判。例如,伪装成科研协作信息的钓鱼邮件、加密实验室核心数据的勒索软件等,部分攻击直接瞄准未发表的研究成果和专利技术。

1.2 内部风险防控难度大

内部人为风险源于多方面,既有人员有意违规操作,如拷贝敏感数据谋取私利、离职后未按保密规定保密数据;也有无意疏忽,如使用弱密码、误点恶意链接、违规传输数据等,给黑客暴力破解、非法入侵留下可乘之机;有的人在日常工作中缺乏警惕性,误点伪装成学术资源、协作通知、会议邀请的恶意链接,或打开附带恶意代码的邮件附件,导致终端设备被植入木马、病毒等恶意程序;还有的违规通过未加密的公共云盘、私人邮箱、社交软件传输敏感科研数据,或随意接入不明公共Wi-Fi开展工作,使得数据在传输过程中易被黑客拦截窃取,最终引发数据泄露事件,间接影响实验室科研、检测等核心业务的正常推进。

1.3 网络安全管理制度缺失

科研人员普遍存在安全意识薄弱、重视程度不够、应急处置能力不足等问题,这就需要专业的管理和技术指导,制定实验室网络信息安全管理制度。部分实验室在管理方面缺乏明确的规范和流程,无法有效应对安全威胁,例如没有明确的网络安全策略、保密规定和应急响应计划等,这使得实验室在发生安全事件时难以及时有效地处置,严重削弱了实验室信息安全管理能力。

2 实验室数智化转型中网络信息安全的核心重要性

2.1 保障科研数据安全

科研数据的原始性、完整性是实验结论的核心支撑。数智化转型中原始数据集中存储、在互联网中传输、自动化采集数据等数据共享、跨终端访问需求行为,极易造成数据丢失、篡改、泄露、污染等风险。若原始数据受到影响,将直接破坏实验室研究成果的完整性与独家性,引发科研项目延期或研究失败,损害实验室人员或团队的学术公信力。

2.2 保障业务连续性

实验室需要防范与规避安全事件引发的业务停摆,保障科研、检测、生产等核心活动的持续推进,同时缩短安全事件后的业务恢复周期,降低延误风险与经济损失。实验室的科研、检测等活动具有连续性、不可逆性等特征,安全事件的发生往往会引发连锁负面影响。一方面,网络攻击可能突破实验室网络防护体系,恶意篡改实验设备控制系统程序、使数智化管理平台陷入瘫痪;另一方面,硬件故障也会直接导致实验仪器停机、数据存储服务器离线,进而造成核心业务中断,最终造成损失。

2.3 提升合作竞争力

跨机构、跨区域科研协同合作能够提高科研竞争力,通过安全合规的协同环境,打破数据共享与合作壁垒,拓展科研资源整合范围,促进科研数据更好地服务于合作互联。

3 实验室信息安全的保障策略

3.1 完善实验室信息安全管理制度

明确科研、运维、管理等各岗位安全职责,形成“责任到岗、分工明确”的管理格局。将业务连续性要求深度融入安全管理,明确安全事件下的业务优先级排序与保障流程,确保科研、检测等核心业务不中断。对标相关法律及行业安全标准,建立合规自查与风险评估机制,定期排查数智化转型中的合规漏洞。采用“PDCA循环”构建闭环管理流程,根据数智化技术迭代与安全风险变化,持续优化管理体系,提升适配性与有效性。依据ISO 27001《信息安全管理体系》等国际标准,建立符合实验室实际的安全管理框架。

3.2 提升实验室人员信息安全意识

开展分层分类安全培训,针对科研人员重点讲解数据加密、隐私保护、实验数据规范存储等内容,为设备运维人员设计智能设备漏洞修复、控制系统防护等专项课程,为管理人员强化安全责任与合规管理培训。组织场景化实操演练,模拟钓鱼邮件攻击、数据泄露应急处置、勒索软件防御等真实场景,提升人员实际应对能力。通过张贴安全警示海报、定期推送典型案例、举办安全知识讲座、举办知识问答竞赛、利用网络平台集体学习等形式,营造“人人重安全、事事讲安全”的文化氛围,强化全员网络安全意识。

3.3 制定应急响应计划

实验室管理者应在应急响应计划中明确应急响应全流程,划分预警、处置、恢复、复盘四个阶段,细化各阶段责任主体、操作步骤与时间节点,确保应急处置有序高效。管理者应编制多场景专项应急预案,针对数据泄露、系统瘫痪、智能设备入侵、核心业务中断等不同安全事件,制定差异化处置方案,明确应对措施与资源保障。组建专业应急响应团队时,应吸纳安全技术人员、业务骨干、管理人员参与,明确各成员分工与协作机制,提升应急处置专业性。

实验室每年至少组织一次应急演练,模拟发生网络安全事件时,应急预案的可行性与团队响应能力,演练后全面复盘,优化预案流程与处置措施。建立改进机制,在安全事件处置后,深入分析事件成因、影响范围与处置效果,总结经验教训,同步优化防护措施。

3.4 升级与优化软硬件设施

实验室中的某些老旧软硬件设施往往因服役年限较长、技术架构相对陈旧,存在显著的安全短板。一方面,部分老旧系统已超出厂商技术支持周期,不再提供安全补丁更新与漏洞修复服务,长期积累的未修复系统漏洞,易被黑客通过自动化扫描工具精准识别并利用,成为突破实验室网络防护体系的“突破口”;另一方面,老旧软硬件与实验室新增的数智化设备、云端协同平台、科研数据分析工具等可能存在兼容缺陷,导致数据传输中断、系统运行不稳定等问题,甚至间接引发安全防护功能失效,为黑客实施注入攻击、远程控制等操作创造可乘之机。

升级与优化软硬件设施更能精准适配当前日益复杂的新型安全威胁防护需求。新设备通常具备更强的识别、拦截与抵御

能力。同时,新设备在兼容性、扩展性上更具优势,适配更多业务场景。

3.5与外部安全服务商合作

实验室应该与网络信息安全专业能力更强的外部安全服务商合作,开展常态化安全风险评估与合规审计,外部第三方审计可为实验室提供客观评估与建议,精准识别数智化转型中的潜在安全隐患。制定应急响应计划时,应该与外部安全服务商进行深入交流,借鉴其专业经验。当遭遇重大网络攻击、复杂安全事件时,借助外部安全服务商的应急响应团队与技术资源,快速处置安全危机,缩短业务中断时间。定期参与外部服务商组织的行业交流与技术培训,及时掌握网络安全前沿技术、行业安全动态与合规政策变化,助力实验室安全防护体系持续迭代升级。

4 结论

实验室数智化转型的深度与广度持续拓展,网络安全的内涵与边界也在不断延伸。面对日益严峻的网络信息安全形势,实验室管理人员需重视网络信息安全管理,通过完善相关管理制度、提升实验室人员安全意识、制定应急响应计划、升级与优化软硬件设施、与服务商合作等方式,实现安全与发展的协同并进,才能真正发挥数智化转型的核心价值,为科研创新活动筑牢安全屏障,推动实验室在科技竞争中持续保持核心优势,

实现高质量、可持续的发展。

[基金项目]

海关总署科研项目(2024HK239)。

[参考文献]

- [1]董军,李旭晨,陈平.网络安全视角下的高校信息安全管理策略研究[J].公关世界,2025,(20):8-10.
- [2]周铭.企业保密工作中信息安全的重要性探讨[J].电信快报,2025,(09):46-48.
- [3]刘滨,顾星海,宋歌.高校化学实验室信息化安全管理体系的建设探讨[J].化工管理,2020,(25):103-104.
- [4]谭敏清,贺鹏艳.关于检验检测实验室在网络数据安全风险管理方面的现状与思考[J].中国标准化,2025,(07):197-201.
- [5]郭皓.计算机网络信息安全管理的重要性[J].电子技术与软件工程,2021,(02):251-252.
- [6]韩一嫡,赵晶磊.浅析信息化安全在企业管理中的重要性[J].电子技术与软件工程,2015,(20):222.

作者简介:

钱仪嘉(2001--),女,汉族,北京人,本科,助理工程师,主要从事信息化和网络安全工作。