证券代码:000004　证券简称:国华网安　公告编号:2025-017

深圳国华网安科技股份有限公司

【2024】年度报告摘要

一、重要提示

本年度报告摘要来自年度报告全文,为全面了解本公司的经营成果、财务状况及未来发展规划,投资者应当到证监会指定媒体仔细阅读年度报告全文。

所有董事均已出席了审议本报告的董事会会议。

非标准审计意见提示

□适用 √不适用

董事会审议的报告期利润分配预案或公积金转增股本预案

□适用 √不适用

公司计划不派发现金红利,不送红股,不以公积金转增股本。

董事会决议通过的本报告期优先股利润分配预案

□适用 √不适用

二、公司基本情况

1、公司简介

股票简称	国华网安	股票代码	000004
股票上市交易所	深圳证券交易所		
联系人和联系方式	董事会秘书	证券事务代表	
姓名	阮旭明		
办公地址	深圳市福田区梅林街道孖岭社区第丰路10号翠林大厦12层		
传真	(0755)83821727		
电话	(0755)83821596		
电子信箱	nanxun@szv000004.cn		

2、报告期主要业务或产品简介

公司作为国内移动应用安全头部企业,积极响应国家“数字经济”的发展战略,认真钻研各类移动应用安全技术,研讨和分析各种互联网移动应用场景,经过多年的精耕细作,初步形成了独有的业务生态体系,从满足单项安全或合规需求的工具类产品,到集成多种功能的平台类产品及覆盖多领域的安全咨询服务,公司能够为客户提供全方位、一站式的移动安全全生命周期解决方案,打造和谐、强大、高度安全的万物互联生态环境。

(一)移动应用安全工具类产品和服务

移动应用安全工具类产品和服务能力贯穿了移动应用设计指引、安全开发测试、应用优化、应用安全发布及应用上线运营阶段的整个生命周期,并拥有丰富的产品形态和高度的业务适配性,用户遍及金融、运营商、政府、电商、能源、教育、游戏等多个行业。

1、安全检测产品:适用于移动应用的开发者客户及各类移动应用持续监督管理者,基于人工智能AI以及大数据技术,借助逻辑推理能力以及外部风险面管理,提升检测引擎研判能力,全面检测移动应用中存在的安全漏洞、编码缺陷、个人信息安全等问题,并出具专业的安全检测报告,对发现的问题给予详细的解决建议,帮助开发者提前避免因安全漏洞导致的安全事故,及时预防安全风险,同时使得检测整改后的移动应用能够满足国家移动应用安全相关法律法规和监管要求。产品采用静态检测、动态检测、内容检测等技术,包括Android应用检测、iOS应用检测、鸿蒙APP检测、SDK检测、个人信息安全检测、微信公众号检测、微信小程序检测、内容检测、固件检测等系列。

2、安全加固产品:适用于移动应用的开发者和运营者客户,能够解决移动应用本身存在的脆弱性问题,有效防止移动应用被破解和篡改等风险发生,保障应用开发者和运营者的合法权益,并在保证安全性的同时兼顾性能,把加固行为对应用安装和运行的用户体验影响降到最低。产品综合采用Android Dex加固、SO加固、SDK加固、输入输出信息保护、密钥自盒、协议加密、C/C++/OC/swift源码混淆保护、Java2CPP保护以及SO Linker等技术,通过第八代All-In VMP加固技术,为用户提供全面的移动应用加固和攻击防范工具及安全套件。

3、个人信息保护产品+服务套件:公司紧密结合个人信息保护法律体系监管要求和企业端的业务需求,推出移动应用个人信息安全检测平台和个人信息安全合规测评服务,其中:个人信息安全检测平台主要针对移动应用的基本信息、漏洞信息、收集和使用个人信息行为、通讯传输行为、软件和技术供应链情况、技术脆弱性、隐私政策规范性等进行多维度安全检测和合规检测,能够帮助监管机构准确、有效地提供行政执法依据,帮助测评机构出具专业的个人信息测评报告,帮助应用市场实现应用上架前的合规风险扫描与控制,帮助应用开发企业在应用发布前评估个人信息的安全性和合规性;同时借助人工智能AI大模型能力,为用户提供全面的个人信息智能客服,以及更强的AI遍历覆盖能力,提升产品以及服务能力。此外,公司提供个人信息合规测评服务,着力解决APP违规收集使用个人信息、过度索权等用户关心的信息安全问题,对标监管机构的通报执行范围、应用市场的合规风险扫描范围、竞品企业的违规测评认定范围等制定合规差距评估模型,提供测评与整改咨询的服务,推进APP合规运营,为移动应用用户的个人信息安全保驾护航。

4、移动应用深度安全-人工服务:利用人工手段协助国家和区域安全监管机构、测评机构、重要行业用户,对现有安全体系和技术手段进行有效补充和完善,服务内容涵盖攻防渗透、隐私合规测评、源代码审计、安全培训、兼容性测试、等级保护安全咨询等,为行业高端用户提供全方位治理服务。一是提供人工渗透服务,在合法且取得用户授权的前提下,通过模拟黑客攻击对整个应用系统进行全面的漏洞检测与分析,输出专业的渗透测试报告,并提出漏洞修复建议与修复指导方案;二是提供高端定制化隐私合规测评服务,帮助企业快速满足国家、监管机构及企业自身的合规政策和标准要求;三是提供源代码审计服务,全面挖掘出应用系统源代码中存在的安全漏洞、性能缺陷、编码规范缺陷等问题,避免因软件代码存在安全漏洞导致的安全事故及风险;四是提供安全培训服务,为客户定制个性化的安全培训课程方案,通过新颖、专业、详细的安全课程培训、安全事件解读与实操实训,帮助企业人员了解并掌握相关安全知识、安全技能;五是提供兼容性测试服务,对移动应用原包及加固包的兼容性(安装、启动、运行、卸载成功率及失败率)、性能(安装、启动耗时、内存占用、CPU占用、流量消耗量)和业务功能可用性进行测试;六是提供等级保护安全咨询服务,结合行业特点对业务信息系统提供定级参考建议,协助客户完成定级备案工作,提供等级保护和安全意识的培训服务。

(二)移动应用安全平台类产品和方案

1、移动应用安全大数据平台:面向移动应用发布运营后监测安全问题的平台级产品,其客户覆盖行业监管、业务运营和各级执法单位。平台利用强大的网络爬虫能力采集各渠道发布的应用,运用内置AI机器智能学习模型自动对海量数据进行规则清洗打标,形成按照区域、行业、功能、特征标签,通过调用平台100多个各类检测引擎将移动应用基础安全防护和检测能力进行有效整合,内置安全评估模型定性、定量客观呈现移动应用安全运行状态和水平,对各种类型移动应用提供主动、持续、动态的风险业务识别、侦测和分析,能够提供指定移动应用运行安全状态监测服务,辅助监管单位对辖区内移动应用进行监测与管理,为移动应用运营单位提供移动应用安全、平稳、合规运行的安全风险分析和能力支撑,并提供必要的决策分析支撑,同时能够根据行业用户需求分别针对企业用户和监管机构推送多种形式的移动应用安全监测数据。

2、移动安全管理平台:客户群体多为行业用户及安全管理部门,平台以企业移动业务安全为核心,结合企业安全策略动态调配自有或第三方安全工具和防护措施,针对监管合规、安全建设、风险管控等业务场景,提供应用检测、应用加固、态势感知、个人隐私检测、内容检测、源代码审计、EMM在内的多种安全能力,基于规划、设计、开发、测试、上线、运营全生命周期,实现移动业务的事前安全管控、事中威胁监测、事后安全管理,帮助企业构建完整的移动安全管理体系,满足企业移动安全体系化建设需求。

3、应用安全风险监测平台:为企业用户实时监测渠道上的Android、iOS、小程序、公众号资产是否存在盗版仿冒风险、通报风险、漏洞风险、个人信息风险、恶意风险、境外传输风险,以及内容安全风险等。平台实时监测超过2000+个主要应用分发渠道,分析应用发布有效性、运营数据全面性而推出的大数据类产品,能够针对各类风险问题进行分析后给出合理化处理建议,并提供专业的安全咨询及整改服务,帮助企业及时规避各项风险,并提供持续性监测能力。

4、移动威胁态势感知平台:针对关注移动应用上线后运行状况和各类安全攻击突发事件的行业客户提供的安全事件监测平台,具备移动应用安全持续监控能力,能够及时发现各种攻击威胁、异常行为、环境风险,实时收集移动应用在使用过程中的安全信息,通过大数据技术对安全事件进行事前态势感知、事中实时响应、事后追踪溯源,对威胁相关的影响范围、攻击路径、目的、手段进行快速判别,提供有效的安全决策和响应建议,并建立安全预警机制和生成威胁风险报告,从而帮助企业安全管理人员掌握移动业务的整体安全态势。

(三)移动安全合规创新产品建设

1、欺诈风控平台

欺诈风控平台是一款针对于移动应用欺诈风险的管理平台,通过有效检测常见涉诈场景,如基于共享屏幕、远程协作、屏幕录像和语音通话发起的欺诈攻击行为,规避业务欺诈损失,同时利用人工智能分析模型,根据授权的软件列表信息与后台反诈数据联动,识别和预警潜在的欺诈风险。通过欺诈防控手段,该产品能够助力用户及时规避涉诈攻击行为,增强业务反诈能力。此外,该产品还能收动应用对业务操作进行风险预警和响应,构建从内至外的业务反诈免疫能力,确保业务安全稳定运行。

2、数据与个人信息合规智探大模型一体机

专为移动应用数据及个人信息合规打造的大模型一体机,融合了国内领先的推理大模型技术框架与算法,在时效性和准确性上大幅提升,同时确保合规检测的智能化和安全性,通过深度整合大模型安全机制,增强数据处理的稳健性和隐私保护能力,严格遵循监管合规要求。产品基于丰富的合规经验数据进行深度学习与优化,智能检测引擎能够动态调整逻辑与参数,保持合规实践的领先地位。

通过政策法规深度融合技术,系统能够自动学习并适应最新合规法规,高效训练 LLM (Large Language Model)大语言模型, 构建全面精准的移动安全合规知识库, 显著提升工作效率。此外, 智能化合规交互助手运用 NLP (Natural Language Processing) 自然语言处理技术,深入理解用户需求,提供人性化、高效的交互体验。结合深度分析与大模型安全保障,该一体机不仅提升了合规检测的智能水平,还确保了流程的安全性与合规性,为用户的数据保护与个人信息合规工作提供坚实的技术支撑。

3、移动应用风险监控大模型一体机

本产品适用于企业自身的移动应用互联网外部暴露风险预警和处置,集成大数据分析引擎,深入剖析移动应用资产发布的各类渠道,能够从海量数据中提取有价值信息。结合最新的《网络安全法》《数据安全法》《个人信息保护法》及各行业部门的法规要求,利用AI技术构建多样化的预判类模型、描述型模型,识别并报告应用的漏洞风险、仿冒盗版活动、合规性违规以及恶意篡改威胁。

基于NLP自然语言分析,构建深度神经网络模型,能够自动学习文本中的深层特征表示,从而实现对自然语言更精确的理解和处理,满足文本分类、信息抽取、搜索引擎多种场景。通过不断自我学习与数据管理,能够持续不断识别外部风险变化的数据,优化丰富风险知识库,从而实现潜在风险的精准风险捕捉,确保企业在第一时间掌握风险状况,采取有效措施减少潜在损失。通过人机交互实现“一问一答”的沉浸式风险观测,满足多场景下的使用体验。

4、移动应用软件成分分析系统

移动应用软件成分分析系统(Mobile Software Composition Analysis, MSCA)基于识别和管理移动应用中使用第三方库和开源组件的技术,主要通过分析移动应用的开源组件以及依赖关系,获取组件安全漏洞、许可证等信息,从而有效地帮助安全开发人员消除应用中的漏洞、违禁协议,减少安全隐患,分析范围主要包括安卓,iOS,鸿蒙等移动应用平台的应用软件包,以及移动SDK,SO文件,小程序,H5程序包等。相比通用软件供应链安全产品,移动应用软件做为更频繁使用的业务访问入口,其运行环境各异,供应链安全缺陷或漏洞更容易被利用。该系统可以赋能移动应用开发企业,强化移动应用供应链安全管理,降低移动应用中使用开源组件的风险。

(四)移动应用安全生态环境建设

公司积极参与国家、行业主管部门和检测测评机构针对移动应用安全发起的专项课题研究、标准编制、新业务试点工作,推动国内移动应用安全生态环境的良性发展,形成政府、企业和用户于一体的互联网安全生态。作为移动应用安全的引领者,公司将通过领先行业的移动安全技术,推动产业互联网、政府互联网、消费互联网的移动应用安全生态的发展,以业务创新实现产业共赢。

除此以外,公司基于在移动安全方面的技术沉淀,积极开拓数据安全相关业务,并通过加强与合作伙伴的合作,进一步向安全开发管理、安全运营、数据安全、物联网、AI安全合规咨询等方向进行拓展。

(五)数据安全咨询服务

该服务包括数据安全治理体系设计、数据安全风险评估等十个类别,涵盖数据安全管理、技术、人员、数据处理活动四个维度,以数据安全监管合规为底线,技术防护为核心,数据安全流转为目标,为企业客户提供专业的咨询服务。

1、数据安全治理体系设计:涵盖数据安全组织架构、管理制度、技术体系、运营体系和文化建设等方面的咨询服务,协助企业建立多方参与的数据安全机制,打通部门间沟通障碍,夯实数据安全治理工作,形成完善的制度、技术防护和运营体系,统一企业内部数据安全共识,实现一体化的数据安全建设,确保企业数据得到有效保护和合法利用。

2、数据安全风险评估:通过识别企业数据泄漏、破坏、窃取、篡用等风险点,以及识别新技术应用(如:5G、人工智能、云计算、大数据等)衍生的新型安全风险,提供有效的安全防护建议;规整国家层面、特定行业层面数据安全风险评估要求,协助企业落实风险评估工作,并构建自评估能力。

3、数据出境安全评估:通过识别企业数据跨境行为及数据内容,厘清企业出境数据详情;精准识别豁免场景,紧贴跨境服务贸易及特定自由贸易试验区负面清单机制,完成数据出境风险评估,清晰掌握出境数据流向及风险,协助企业编写符合网信办数据出境安全评估申报表、出境风险自评估报告,辅助完成申报工作。

4、个人信息保护咨询服务:基于《中华人民共和国个人信息保护法》《个人信息保护合规审计管理办法(征求意见稿)》和《数据安全技术 个人信息保护合规审计要求(征求意见稿)》,对企业各项业务中的个人信息处理过程进行调研,梳理个人信息和业务逻辑流转情况,识别目标信息数据;对于重点场景个人信息保护现状开展全面风险评估,并对前台涉及个人隐私的重点系统进行个人隐私设计评估,定位企业在个人信息治理、管理、技术层面存在的漏洞与不足,提出治理、产品设计、系统控制等层面的整改优化建议,并开展持续的跟踪督办工作。

5、数据安全认证评估咨询:协助企业选择适合的数据安全管理能力认证证书,全面衡量企业数据安全能力成熟度,“一站式”协助企业完成DSM(Data Security Management,数据安全管理认证)、DSMM(Data Security Capability Maturity Mode,数据安全能力成熟度认证)、DCMM(Data Management Capability Maturity Model,数据管理能力成熟度认证)、DSMC(Certificate for Data Security Management Capability,数据安全管理能力认证)对应认证工作,提升企业竞争力。

6、数据安全专业培训:公司拥有丰富的数据安全、个人信息安全监管处罚案例库,能针对不同层级人员进行定制化培训内容输出,建立企业员工对数据安全、个人信息保护的正确认识,规范员工日常行为;打破行业壁垒,让企业充分了解数据安全、个人信息保护最新监管政策及趋势,以便规划合规方案。

7、数据安全应急服务:针对数据安全突发事件预制方案,确保企业及时、有序、有效地开展应急响应工作;结合企业实际业务场景及现行预案流程,制定演练脚本,检查预案的科学性和有效性;通过专业的数据安全应急响应技术人员,提供7*24小时现场支撑;协助客户构建数据安全应急管理机制,满足监管合规要求,有效识别数据安全预案缺陷,增强企业应对突发数据安全事件的信心和应急意识;在重保期间可快速补充内部缺失的专业技能人才。

8、数据分类分级咨询:根据企业所处行业特性对现有数据分类分级框架进行分析,提供统一的分类维度及定级标准建议;结合分级框架梳理策略,优化分类分级工具效率及准确度;协助企业建立适用自身业务特色的分类分级标准,完善数据安全治理基础工程,推动数据分级分管控技术措施落地。

9、数据安全专项检查服务:公司拥有专业的移动应用个人信息检测平台和移动应用安全检测平台,能够辅助企业快速识别移动应用相关风险;通过体系化数据安全评估矩阵,全方位覆盖各监管机构检查维度,帮助企业快速应对专项检查工作,落实数据安全防护义务。

10、应用系统数据安全管控咨询服务:公司拥有丰富的数据安全技术管控基线知识库,可快速结合企业数据安全防护现状提取适用自身的应用系统数据安全管控要求;成熟的应用安全开发管控平台,可以在应用系统全生命周期无缝嵌入数据安全基线;专业的合规及安全测试团队,可以对应用系统数据安全基线进行符合性验证,完成数据安全闭环管理。服务中公司以应用系统作为管控抓手,将数据安全、隐私合规管控要求前置至应用系统需求阶段,从源头解决合规问题及技术保护难题,减少后续风险修复成本;协助企业履行监管及内部数据安全管理要求,推进存量应用系统数据安全风险整改,以及新增应用系统内生数据安全防护。

(六)业务拓展

1、开发安全管理

(1)软件安全开发管理平台:为软件开发团队提供的可持续性贯彻安全策略的辅助平台,以SDL(Security Development Lifecycle安全开发周期)为设计理念,构建覆盖应用开发各环节、工具统一运行调度的管理系统,从立项开始进行安全管理的全程介入,实现了安全左移的管理效果。平台包含了各阶段流程的梳理、相关安全知识库的建设、评审机制的建立,能够兼容多种开发模式,包括自适应瀑布开发模型、敏捷开发模型、DevOps模型等,可针对不同的安全治理诉求,有效地帮助客户建立定制化的安全管理体系,从而推动安全管理流程落地,为各类软件开发企业提供安全赋能。

(2)软件开源组件成分分析系统:主要面向需要管理规模数量较多、拥有自有以及第三方开发软件系统的用户,能够协助软件资产所有者对所拥有的软件产品中的第三方开源组件实施安全管控,帮助企业建立开源技术应用管理制度体系和标准化软件资产台账,实时预警开源组件安全及合规问题,并通过全面可视化统计能力有效提升企业对软件供应链的安全管理能力。

(3)源代码审计系统:提供对目标软件代码语法、语义的分析,辅以数据流分析、控制流分析和特有的缺陷分析,能够高效的检测出软件源代码中的可能导致严重缺陷漏洞和系统运行异常的安全问题和程序缺陷,并准确定位告警,从而有效的帮助开发人员消除代码中的缺陷、减少安全隐患。

2、安全运营类产品

(1)网络安全有效性验证系统(BAS - Breach and Attack Simulation,即入侵和攻击模拟):主要对企业的网络安全防御体系中的安全设备和安全策略进行网络安全有效性验证。由于企业在安全管理、技术方面存在的缺陷,各种安全威胁层出不穷,快速迭代,企业建立网络安全防御体系普遍存在失效的情况,并且失效情况很难被人为发现,如:运维人员配置安全策略问题,安全设备因为性能问题导致丢失数据和告警事件,对特定威胁无防御能力,设备新威胁防护缺失等。该产品通过实战化、体系化、常态化的方式,模拟真实攻击方法和场景,自动化地验证现有的企业安全体系是否存在弱点问题,在企业发生安全事件前,提前进行修复,避免对企业带来业务损失。

(2)运行时应用自免疫系统:主要针对Web应用的运营者客户,采用业内前沿防护理念RASP(Runtime Application Self-protection,运行时应用自我保护),安装过程无需修改任何应用程序自身代码,将Web防护检测引擎注入到应用程序里,与应用程序融为一体,在应用程序运行时可对访问请求做精准分析,实现自我安全保护,减少了传统防护技术分析流量数据带来的误报,识别并拦截新型Web攻击,为应用系统的安全防护提供了创新解决方案,为预防未知移动应用安全风险漏洞提供新型防护手段。

3、数据安全治理

(1)数据安全分类分级系统:是面向企业数据发掘并进行自动化数据分类分级分析的产品。该系统致力于梳理并标识数据,实现在复杂环境下自动化扫描并识别其中的敏感数据信息,在数据的分类分级梳理过程中搭建数据标准,实现数据口径的统一。通过优质且智能化的数据服务扫描能力和敏感数据自动化识别能力,该系统可对海量的数据资产进行扫描和自动化分类分级,实现在基础零业务打扰的情况下,在扫描的同时完成对数据资产的自动化标识。该系统的智能分析引擎以多维度的规则匹配与机器学习能力深度学习企业的数据资产业务场景,形成一套贴合客户实际业务场景的算法模型,使自动化分类分级更精准。同时系统将分类分级结果以多个维度进行可视化呈现,可提供数据清单维度的分级结果、标签分类维度的分级结果、数据分级维度的识别结果。

(2)应用数据审计系统:是一款针对web应用系统的数据安全产品,采用网络流量分析技术,在对现有业务系统无侵入的情况下,帮助客户全面盘点线上业务系统接口,及时发现大规模数据流动风险,快速对数据泄露事件进行溯源分析,宏观掌控业务系统数据流动态势。

(3)数据出境合规治理平台:针对非移动应用数据,提供范围更广的数据出境合规治理服务,适用于被判定为数据出境的管辖对象、希望对出境业务进行安全评估的企业、希望对出境行为进行持续监控的企业和不清楚业务数据是否涉及境外流动,希望进行出境安全检测的企业等。该平台以敏感数据出境治理为核心,帮助企业持续有序地治理出境业务,提供数据出境评估和监测能力,规范数据出境活动以满足合规监管要求。平台遵循“事前评估、事中监测、事后留档”的治理思路,事前对出境资产进行合规风险评估,事中对出境行为变化进行实时监测并将风险事件纳入处置中心,事后可依据实际情况决定是否采纳治理或再次进行评估,生成报告存档以便后期进行对比分析和整改。

4、物联网安全

物联网安全产品主要包括边缘计算算力网关以及物联网终端安全检测平台应用等产品和服务,基于安全基权和加密算法的研发,与运营商深度合作,通过安全网络通道的数据传输,实现物联网设备的安全运营、有效防劫持等。公司在人工智能领域布局,开发人工智能算力管理平台,提升算力建设和运营服务能力,另外开发边缘计算管理平台,实现边缘算法的训练、应用开发和算法部署,通过这两大平台,构建从人工智能开发到应用的完整解决方案。

物联网IOT安全防护平台:随着多种接入网络技术和智能计算技术的飞速发展,智能家居、智慧城市的物联网蓬勃发展,没有经过严格安全设计的IOT设备的远程注入和控制成为新的威胁来源。物联网IOT安全防护平台,依据“逐级分层,边界控制,整体监测”思路,在保证物联网业务运营发展的前提下,基于纵深防御、整体全程数据监测为基本目标,覆盖物联网业务发展全生命周期(规划与咨询、开发与设计、发布与运维)的安全保护;从设备资产、威胁和脆弱性多层次建设,管理层覆盖安全咨询培训以及运营管理,应用层覆盖漏洞安全检测、漏洞加固防护、人验认证识别防护等,网络层提供协议加密安全防护手段保障数据安全加密传输,感知层提供威胁态势实时监测和响应,结合物联网业务特点进行威胁建模,支持复杂决策分析和时序分析,有效防范物联网IOT相关的攻击行为风险。

5、AI安全合规咨询

(1)AI安全治理咨询服务:致力于协助企业构建多元主体参与的AI安全合规治理机制,明确治理目标,归纳相关法规政策、标准规范,采用敏捷治理模式,通过技术支撑、监测评估、管理措施等多类措施,促进AI安全合规和健康发展。

(2)AIGC(算法/模型)备案咨询服务:旨在协助企业完成算法/模型备案流程,包括资料准备、系统填报、审核跟进等,确保企业合规运营,避免法律风险。

(3)AIGC合规评估服务:对企业生成式人工智能(AIGC)项目进行全面合规性检查的服务,旨在确保项目符合模型安全、语料合规、内容符合伦理等要求,助力企业合规发展。

(4)AI合规意识培训服务:专注于增强企业团队对AI技术的合规理解,包括最新法律法规、伦理原则及行业最佳实践,旨在培养全面的合规观念,推动企业内部形成坚实的AI合规文化氛围。

6、智慧车联

智慧车联产品主要包括汽车电子智能终端、车联网等产品。汽车电子智能终端包括智能行车记录仪、智能360环视等后装产品以及无线360环视、(行人和碰撞检测)双预警方案等前装产品;产品目前主要应用于行业平台客户,通过摄像头感知、AI算法、大数据,为平台客户提供监管监控服务,优化运营效率。

7、医疗信息化

公司医疗信息化业务主要聚焦在智慧医疗服务、移动医疗应用安全和医疗分类分级数据治理。智慧医疗服务方案涵盖智慧病房构建及智慧医院评价咨询服务;移动医疗应用安全方案专注于个人隐私保护合规、移动应用的安全检测与防护;医疗分类分级数据治理方案助力医疗机构实现高效的数据管理和价值挖掘。

8、新能源产业综合能源管理服务

主要业务形态为新能源产业的综合能源管理及服务,以目的地智能充放电等为核心业务,包括新能源四轮汽车充电桩、两轮电动车充电桩等智能充、放电项目建设;集中式、园区分布式光伏、储能及能源管理等节能方案设计及项目建设和运维。

(八)医药研发业务

报告期内,公司完成了对合肥拓锐的增资,增资后持有合肥拓锐51%的股权。合肥拓锐专业从事化学药品研发,具备较强的研发能力,累计研发项目二十余项,获批十余项。合肥拓锐研发产品涵盖原料药、普通口服固体制剂、注射液等多种剂型。

3、主要会计数据和财务指标

(1)近三年主要会计数据和财务指标

公司是否需追溯调整或重述以前年度会计数据

□是 √否

单位:元

	2024年末	2023年末	本年末比上年末增减	2022年末
总资产	311,208,761.20	413,449,330.43	-24.73%	576,732,674.01
归属于上市公司股东的净资产	64,038,621.94	195,574,037.27	-67.26%	352,567,397.22
	2024年	2023年	本年比上年增减	2022年
营业收入	98,660,353.71	110,048,548.32	-10.35%	166,463,228.95
归属于上市公司股东的净利润	-131,535,415.33	-156,992,891.72	16.22%	-595,037,295.43
归属于上市公司股东的扣除非经常性损益的净利润	-124,233,068.26	-138,275,037.96	10.16%	-591,816,320.23
经营活动产生的现金流量净额	-16,671,888.17	-36,060,910.29	53.75%	-33,142,088.42
基本每股收益(元/股)	-0.9936	-1.1859	16.22%	-4.0857
稀释每股收益(元/股)	-0.9936	-1.1859	16.22%	-4.0857
加权平均净资产收益率	-101.33%	-57.28%	-44.05%	-91.52%

(2)分季度主要会计数据

单位:元

	第一季度	第二季度	第三季度	第四季度
营业收入	15,450,083.67	21,607,615.35	38,776,677.83	22,765,976.86
归属于上市公司股东的净利润	-10,752,477.74	-8,252,379.23	-16,821,188.08	-98,708,660.28
归属于上市公司股东的扣除非经常性损益的净利润	-10,769,137.80	-8,593,709.32	-13,816,172.59	-91,054,048.55
经营活动产生的现金流量净额	-4,886,171.71	-13,241,691.05	-5,691,467.27	7,147,441.86

上述财务指标或其加总数是否与公司已披露季度报告、半年度报告相关财务指标存在重大差异

□是 √否

4、股本及股东情况

(1)普通股股东和表决权恢复的优先股股东数量及前10名股东持股情况表

单位:股

报告期末普通股股东总数	43,814	年度报告披露日前一个月末普通股股东总数	36,244	报告期末表决权恢复的优先股股东总数	0	年度报告披露日前一个月末表决权恢复的优先股股东总数	0
前10名股东持股情况(不含通过转融通出借股份)							
股东名称	股东性质	持股比例	持股数量	持有有限售条件的股份数量	质押、标记或冻结情况		
					股份状态	数量	
深圳中农大科技投资有限公司	境内非国有法人	18.29%	24,206,848	0	不适用	0	
北京中关村并购母基金投资管理中心(有限合伙)-北京中关村并购母基金投资中心(有限合伙)	其他	4.00%	5,296,206	0	不适用	0	
彭赢	境内自然人	3.29%	4,356,845	4,356,592	冻结	4,356,845	
					质押	2,811,300	
深圳市睿鸿置业发展有限公司	境内非国有法人	3.03%	4,015,934	0	不适用	0	
魏巍	境内自然人	2.68%	3,553,722	0	不适用	0	
珠海横琴普君科技合伙企业(有限合伙)	境内非国有法人	2.53%	3,356,306	0	不适用	0	
李映彤	境内自然人	0.99%	1,316,100	0	不适用	0	
郭训平	境内自然人	0.59%	787,486	787,486	冻结	787,486	
					质押	787,486	
郑州众合网安信息科技有限公司	境内非国有法人	0.34%	450,337	450,336	冻结	450,337	
					质押	450,000	
杨光	境内自然人	0.34%	447,000	447,000	不适用	0	
上述股东关联关系或一致行动的说明	深圳中农大科技投资有限公司的实际控制人李映彤与深圳市睿鸿置业发展有限公司及珠海横琴普君科技合伙企业(有限合伙)的实际控制人李映彤系近亲关系;彭赢曾持有郑州众合网安信息科技有限公司7.6190%股权并担任法定代表人,郭训平持有郑州众合网安信息科技有限公司20.5882%股权。此外,公司未知上述股东中其他股东之间是否存在关联关系,也未知其是否属于《上市公司收购管理办法》规定的一致行动人。						
参与融资融券业务股东情况说明(如有)	李映彤通过信用证券账户持有公司股份1,210,000股。						

持股5%以上股东、前10名股东及前10名无限售流通股股东参与转融通业务出借股份情况

□适用 √不适用

前10名股东及前10名无限售流通股股东因转融通出借/归还原因导致较上期发生变化

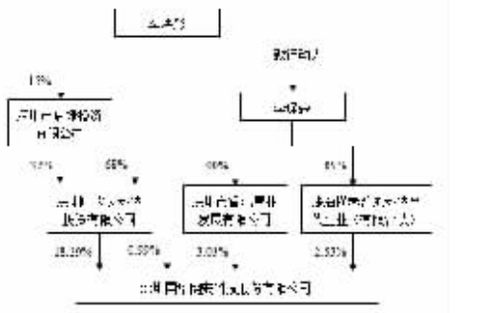
□适用 √不适用

(2)公司优先股股东总数及前10名优先股股东持股情况表

□适用 √不适用

公司报告期无优先股股东持股情况。

(3)以方框图形式披露公司与实际控制人之间的产权及控制关系



5、在年度报告批准报出日存续的债券情况

□适用 √不适用

三、重要事项

1、《公司章程》修订

公司根据2023年12月发布的《上市公司章程指引》和《上市公司监管指引第3号——上市公司现金分红》等有关规定及公司实际情况,对《公司章程》部分条款进行修订,详见公司于2024年4月30日披露的《关于修订(公司章程)的公告》(公告编号:2024-009)。上述修订已经公司董事会和股东大会审议通过,详见公司于2024年4月30日披露的《第十一届董事会第四次会议决议公告》(公告编号:2024-004)和5月28日披露的《2023年年度股东大会决议公告》(公告编号:2024-020)。

2、董监高变动

报告期内,公司独立董事仇夏萍女士提出辞职,公司选举孙俊英女士为新任独立董事,详见公司于2024年5月8日披露的《关于独立董事辞职的公告》(公告编号:2024-013)、10月26日披露的《关于提名独立董事候选人的公告》(公告编号:2024-037)和11月12日披露的《2024年第一次临时股东大会决议公告》(公告编号:2024-044)。

公司监事长李钰女士提出辞职,经控股股东提名,公司选举叶鹏先生为监事长,详见公司于2024年5月14日披露的《关于监事长辞职的公告》(公告编号:2024-014)、5月18日披露的《关于增加2023年年度股东大会临时提案暨补充通知的公告》(公告编号:2024-019)、5月28日披露的《2023年年度股东大会决议公告》(公告编号:2024-020)和8月23日披露的《第十一届监事会第五次会议决议公告》(公告编号:2024-025);公司监事逄亚琪女士提出辞职,经控股股东提名,公司选举赵联国先生为新任监事,详见公司于2024年12月4日披露的《关于监事辞职的公告》(公告编号:2024-054)、《关于增加2024年第二次临时股东大会临时提案暨补充通知的公告》(公告编号:2024-055)和12月14日披露的《2024年第二次临时股东大会决议公告》(公告编号:2024-057)。

公司副总经理付志伟先生、财务总监陈金海先生、总经理黄翔先生分别提出辞职,公司聘请于青川先生为副总经理、吴涤非先生为财务总监,详见公司于2024年3月21日披露的《关于高级管理人员辞职的公告》(公告编号:2024-002)、5月18日披露的《关于聘任高级管理人员的公告》(公告编号:2024-017)、10月26日披露的《关于高级管理人员辞职的公告》(公告编号:2024-041)和11月13日披露的《关于总经理辞职及聘任财务总监的公告》(公告编号:2024-047)。

此外,由于董事和高级管理人员变动,公司对董事会部分专门委员会的委员进行了调整,详见公司于2024年11月13日披露的《第十一届董事会2024年第三次临时会议决议公告》(公告编号:2024-045)。

3、对合肥拓锐生物科技有限公司增资

报告期内,公司全资子公司深圳市国华智健医药科技有限公司(以下简称“国华智健”)与合肥拓锐生物科技有限公司(以下简称“合肥拓锐”)签署了《关于合肥拓锐生物科技有限公司之增资协议》,国华智健以1,271.8574万元对合肥拓锐进行增资,增资完成后,国华智健持有合肥拓锐51%股权,具体内容详见公司于2024年12月25日披露的《关于对合肥拓锐生物科技有限公司增资的公告》(公告编号:2024-060)。截至2024年12月30日,国华智健已向合肥拓锐支付全部增资价款1,271.8574万元,合肥拓锐已完成本次增资的工商变更登记手续,并取得由合肥市市场监督管理局换发的《营业执照》,具体内容详见公司于2025年1月2日披露的《关于对合肥拓锐生物科技有限公司增资的进展公告》(公告编号:2025-001)。

证券代码:000004　证券简称:国华网安　公告编号:2025-016

深圳国华网安科技股份有限公司
第十一届监事会第六次会议决议公告

本公司及监事会全体成员保证信息披露的内容真实、准确、完整,没有虚假记载、误导性陈述或重大遗漏。

一、监事会会议召开情况

深圳国华网安科技股份有限公司(以下简称“公司”)第十一届监事会第六次会议于2025年4月28日在深圳市福田区梅林街道孖岭社区凯丰路10号翠林大厦12层会议室以现场和通讯表决的方式召开。会议通知于2025年4月18日以电子邮件形式发出。会议由公司监事长许垂斌先生主持,应到监事3名,实到3名。本次会议的召开符合《公司法》和《公司章程》的有关规定。

二、监事会会议审议情况

1、审议通过《2024年年度报告及摘要》。

经审核,监事会认为董事会编制和审议深圳国华网安科技股份有限公司2024年年度报告的程序符合法律、行政法规及中国证监会的规定,报告内容真实、准确、完整地反映了上市公司的实际情况,不存在任何虚假记载、误导性陈述或者重大遗漏。

具体内容详见公司同日披露的《2024年年度报告》和《2024年年度报告摘要》(公告编号:2025-017)。

表决情况:3票同意,0票反对,0票弃权。

本议案需提交股东会审议。

2、审议通过《2024年度监事会工作报告》。

具体内容详见公司同日披露的《2024年度监事会工作报告》。

表决情况:3票同意,0票反对,0票弃权。

本议案需提交股东会审议。

3、审议通过《2024年度财务决算报告》。

具体内容详见公司同日披露的《2024年年度报告》第十节 财务报告。

表决情况:3票同意,0票反对,0票弃权。

本议案需提交股东会审议。

4、审议通过《2024年度权益分派预案》。

监事会认为,公司2024年度权益分派预案符合中国证监会《上市公司监管指引第3号——上市公司现金分红》及《公司章程》等有关规定关于利润分配的要求,充分考虑了公司实际经营状况及未来发展需要,不存在损害公司及全体股东尤其中小股东利益的情形。

具体内容详见公司同日披露的《关于2024年度拟不进行利润分配的公告》(公告编号:2025-018)。

表决情况:3票同意,0票反对,0票弃权。

本议案需提交股东会审议。

5、审议通过《2024年度内部控制评价报告》。

监事会认为,公司根据内部控制的基本原则建立了较为完善和有效的内部控制体系,符合国家相关法律法规要求以及公司生产经营管理实际需要,并能得到有效执行。公司内部控制评价报告真实、客观、准确地反映了公司内部控制制度的建设及实际运行情况。

具体内容详见公司同日披露的《2024年度内部控制评价报告》。

表决情况:3票同意,0票反对,0票弃权。

本议案需提交股东会审议。

6、审议《关于监事薪酬的议案》。

2024年度,公司监事获得的薪酬情况如下:

序号	姓名	职务	任职状态	税前薪酬(万元)
1