公司代码:688561　　公司简称:奇安信

奇安信科技集团股份有限公司

【2021】年度报告摘要

第一节 重要提示

1 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http://www.sse.com.cn/网站仔细阅读年度报告全文。

2 重大风险提示

公司已在本报告“第三节 管理层讨论与分析”之“风险因素”中说明了可能对公司产生重大不利影响的风险因素,并提请投资者特别关注如下风险:

业绩下滑或亏损的风险

2021年公司营业收入58.09亿元,同比增长39.60%,尤其是布局的新赛道产品、主动防护类产品。公司未来能否保持持续成长,受到宏观经济、产业政策、行业竞争态势等宏观环境等因素的影响,同时公司未来经营业绩也取决于公司技术研发,产品市场推广及销售等因素。市场规模的变化、细分领域的市场竞争加剧、产品更新换代、新市场需求的培育等因素均可能导致下游市场需求发生波动。如果未来公司现有主要产品市场需求出现持续下滑或市场竞争加剧,同时公司未能及时培育和拓展新的应用市场,将导致公司主营业务收入、净利润面临下降的风险。公司将持续在产品研发、市场推广及销售等方面进行投入,如公司收入未能按计划增长,或规模效应未按预期逐步显现,则可能导致亏损进一步增加。如果上述影响公司持续成长的因素发生不利变化,且公司未能及时采取措施积极应对,则不能保证收入按计划增长,公司存在持续亏损的风险,将导致公司存在成长性下降或者不能达到预期的风险。

3 本公司董事会、监事会及董事、监事、高级管理人员保证年度报告内容的真实性、准确性、完整性,不存在虚假记载、误导性陈述或重大遗漏,并承担个别和连带的法律责任。

4 公司全体董事出席董事会会议。

5 信永中和会计师事务所(特殊普通合伙)为本公司出具了标准无保留意见的审计报告。

6 公司上市时未盈利且尚未实现盈利

√是 □否

网络安全产品及技术研发以及销售和服务网络的搭建完善需要大量投入。报告期内,公司净利润为-55,396.97万元,亏损较上年同期增加62.58%,归属于母公司所有者的净利润-55,474.96万元,亏损较上年同期增加65.91%,归属于上市公司股东的扣除非经常性损益后的净利润-78,816.25万元,亏损较上年同期增加46.15%。截止2021年末,公司累计未分配利润为-305,355.27万元。公司持续亏损的主要原因是选择了高研发投入且人员快速扩张的发展模式,为建设研发平台、布局“新赛道”产品、提升攻防竞争力、建立全国应急响应中心而进行了大量投入。首先,研发平台聚焦核心技术能力的平台化输出,为安全产品提供共性核心能力,这些研发平台的开发具有周期长、投入高的特点;其次,公司核心产品主要为网络安全领域的“新赛道”产品,开发这些产品要采用大量新技术,对研发人员能力要求高,增加了公司的研发投入;此外,公司在盈利模式的建设期仍需扩张研发团队和技术支持及安全服务团队,以期夯实规模性研发底座,向客户提供高质量的安全技术服务,积聚品牌效益,产生持续性商机,因此产生大量人员费用。公司尚未盈利且存在累计未弥补亏损,尽管报告期内公司平台已量产,预计研发费用增速会有明显下降,公司各项费用管控措施已实施,营业收入持续高速增长,规模经营效益已逐年提升,未来能否扭亏为赢有不确定性,无法保证短期内实现盈利或进行利润分配。

7 董事会决议通过的本报告期利润分配预案或公积金转增股本预案

公司2021年度利润分配预案为:不派发现金红利,不送红股,不以资本公积金转增股本。以上利润分配预案已经公司第一届董事会第二十八次会议审议通过,尚需公司2021年年度股东大会审议。

8 是否存在公司治理特殊安排等重要事项

□适用 √不适用

第二节 公司基本情况

1 公司简介

公司股票简况

√适用 □不适用

公司股票简况					
股票种类	股票上市交易所及板块	股票简称	股票代码	变更前股票简称	
A股	上海证券交易所科创板	奇安信	688561	-	

公司存托凭证简况

□适用 √不适用

联系人和联系方式

联系人和联系方式	董事会秘书(信息披露境内代表)	证券事务代表
姓名	马勋恩	张鹏
办公地址	北京市西城区西直门外南路26号院奇安信安全中心	北京市西城区西直门外南路26号院奇安信安全中心
电话	010-56500268	010-56500268
电子信箱	ir@qianxin.com	ir@qianxin.com

2 报告期公司主要业务简介

(一) 主要业务、主要产品或服务情况

公司专注于网络空间安全市场,主营业务为向政府、企事业类客户提供新一代企业级网络安全产品和服务。公司创建了面向万物互联时代的网络安全协同联动的主动防御体系,凭借持续的创新研发和以实战攻防为核心的安全能力,已发展成为国内领先的基于安全大数据、人工智能和安全运营技术的网络安全产品及服务提供商。公司面向新型基础设施建设、面向数字化业务,结合“内生安全”思想,将新一代网络安全框架作为顶层设计指导,以“数据驱动安全”为技术理念、以打造网络安全颠覆性和非对称性能力为目标,创建了面向万物互联时代的网络安全协同联动防御体系。公司针对云计算、大数据、物联网、移动互联网、工业互联网和5G等新技术下产生的新业态、新业务和新场景,为政府与企业等机构客户提供全面、体系化的网络安全解决方案。

报告期内,公司主营业务分为网络安全产品、网络安全服务、硬件及其他。

1、网络安全产品

公司将网络安产品分为终端安全、边界安全、数据安全、实战型态势感知四大类安全产品。

终端安全产品,包括面向万物互联场景下的各类终端安全防护产品,如终端安全防护平台、终端安全运营平台、终端环境感知系统、移动终端安全防护系统、工业主机安全防护平台、国产化安全可信浏览器、服务器安全防护系统、云虚拟化安全防护系统等。

边界安全产品,包括防火墙及下一代防火墙、虚拟化防火墙系统、统一威胁管理、Web应用防护系统、入侵防御与检测、VPN安全网关、网闸(数据交换平台)、SD-WAN、边界安全栈等品类。

数据安全品类,包括数据安全态势感知平台、零信任数据安全产品、特权账号管理系统、运维安全管理系统、大数据安全交易沙箱、数据库安全审计与防护、数据防泄漏、源代码安全、APP隐私合规检测平台、电子数据取证等围绕着数据全生命周期以及云、大、移、工场景下的数据安全防护品类。

实战型态势感知产品,包括以安全大数据驱动的十类态势感知平台级产品,即网信态势感知、公安态势感知、工信态势感知、行业监管态势感知、工业互联网态势感知、安全运营态势感知、数据安全态势感知、车联网态势感知、安全攻防态势感知、云场景API安全态势感知。

2、网络安全服务

安全服务系公司根据客户的实际需求,为客户提供的技术、咨询及安全保障等服务,包括安全咨询与规划、评估与测试、分析与响应、订阅式威胁情报与远程托管式安全运营等。

3、硬件及其他

硬件及其他业务系公司在为客户提供体系化网络安全解决方案的过程中涉及到的政企客户信息化配套改造类项目,基于客户需求为客户外采第三方硬件产品并销售给客户的产品及运营服务等业务。

(二) 主要经营模式

1、研发模式

公司秉承“数据驱动安全”的技术理念,以市场需求为导向,坚持自主研发、自主创新,针对不同种类的产品和服务,针对不同客户的多样化需求,打造了独特的研发模式。

公司通过采用“产品(项目)开发+平台研发”的“横向”分层设置,覆盖公司业务开展中的研发场景,避免了通用性功能或模块在不同产品中的重复开发,通过委员会“纵向”技术管理组织,加强公司各类产品、安全平台、工程技术能力建设。两者形成“纵横”协同,保证了公司研发体系有序开展研发工作,能够极大地提高产品研发效率,缩短产品创新周期,降低产品成本,提高产品质量。

2、盈利模式

公司盈利主要来源于为政企客户体系化交付自主研发的网络安全产品,提供安全咨询规划、安全运营等各类安全服务,并满足政企客户在数字化转型过程中所遇到的各类网络安全建设需求。

3、采购模式

公司主要采购两大类软硬件设备,主要包括两大类:一类是公司自有产品所需的服务器、工控机等相关硬件设备;另一类是公司承接网络安全集成类业务所需的第三方软硬件产品及服务。

对于第一类物料的采购,公司建立了相关制度规范采购行为,由商务与供应链中心汇总项目及产品需求,合同订单和产品出货情况,综合考虑公司库存等因素,制定采购计划并实施采购。对于第二类物料的采购,公司主要通过招投标等市场化方式进行,如果客户有明确要求,则会根据其要求进行指定采购。

4、生产模式

(1)安全产品生产模式

公司的产品生产主要包括纯软件模式和软件灌装模式:纯软件模式由公司根据合同约定向客户交付软件;软件灌装模式是将软件产品灌装到外购的硬件设备(工控机、服务器等),再交付给客户。

(2)安全服务模式

安全服务是公司根据客户的实际需求,为客户提供的技术、咨询及安全保障等服务,包括咨询与规划、评估与测试、分析与响应、订阅式威胁情报与远程托管式安全运营等。公司与客户洽谈、沟通达成合作意向后,成立安全服务项目小组开展前期调研、制定服务方案及组织服务的实施工作。

(3)安全集成模式

公司的安全集成业务主要为客户提供包含自有安全产品、安全服务、集成服务和第三方软硬件产品的销售及体系化交付。

5、销售模式

公司的产品和服务的销售采用直接销售与渠道销售相结合的模式。

(1)直接销售模式

对于大中型政企客户,如政府、公安、军队、金融、互联网以及能源、电力、运营商等央企和其他大型企业,公司一般采用直销的方式,安排专门的销售及技术团队为其服务,从而确保与客户持续、稳定的合作,为公司带来长期收益。

(2)渠道销售模式

对中小型客户,公司采取了区域与行业相结合的渠道销售模式,以便最大程度地覆盖更多的客户,提高市场占有率。区域经销体系是全国总经销商与各层级经销商相结合的多层次体系,各层级经销商在市场拓展、渠道建设等方面各有分工;行业渠道商主要覆盖政府、公检法司等重点行业客户,包括经销和项目合作两种模式。区域和行业渠道商根据需求采购公司产品,通常在采购后即交付给最终用户,因此项目合作伙伴的采购一般均有明确的最终用户需求。

(三) 所处行业情况

1. 行业的发展阶段、基本特点、主要技术门槛

2021年,全球网络空间局部矛盾冲突接连不断,现实冲突与网络空间冲突相互交织,在日益不稳定的全球网络安全格局中,大规模针对性网络行动大幅增加,攻击复杂性持续上升,网络安全已成为影响国家安全的重要因素。为此,各国持续加强网络顶层设计、加速网络空间军事竞争、加快网络安全技术赋能,国家级网络安全能力建设正与私营企业技术融合发展,网络强国建设已经从“粗放式”发展延伸至“精细化”耕耘的新阶段。

中国网络安全市场在“十四五”期间逐步迈入高速发展阶段,受益于国家数字经济快速发展,数据已成为第七大生产要素,网络空间安全是数字经济的核心支撑,我国网安产业规模与发达国家相比仍具备很大的成长空间,产业增速将持续领跑全球网络安全市场。具体而言,大数据、云计算、人工智能、5G、工业互联网、车联网等新技术新场景的快速发展,带来更多的安全需求;“十四五”规划中,强调加快推动数字产业化,培育壮大大数据、云计算、网络安全等新兴数字产业,又进一步扩大了需求侧;全行业客户数字化转型、云化转型、智能化转型的加速,让网络安全从传统的本地网络零散式安全建设到覆盖更复杂业务场景全面型体系化安全建设方案转变;俄乌冲突中网络战发挥了关键作用,俄乌战争加速了国内关键信息基础设施行业客户对网络安全实战化、体系化的重视程度,促进了大型政企客户持续加大网络安全建设的预算投入。

目前,网络安全建设正在从“被动式、零散式”安全产品堆砌方案逐步发展为“全面型、体系化、实战化”的主动安全防御方案;以安全服务带动产品方案的销售模式将成为产业发展的新业态,托管式安全运营将成为未来的新安全运营模式,参考海外发达国家的安全产业特性,中国网络安全服务市场的快速发展将成为产业高速发展的重要助力。

一、行业宏观环境持续释放利好,网络安全支出有望大幅增长。

国家安全层面,网络空间安全已成为各国国防安全建设的重要组成部分,是国家关键信息基础设施行业的刚性需求。俄乌战争是人类历史上首次公开、大规模的网络战,已引发全球国家的重要关注,促进国内关键信息基础设施行业客户加大网络空间安全能力建设的预算投入。

经济建设层面,“十四五”时期,我国进入由工业经济向数字经济大踏步迈进的关键时期,经济社会数字化转型成为大势所趋,为推动战略科技创新,确保产业链、供应链安全,国家将会在包括网络安全在内的科技领域继续加大投入。疫情以后的经济振兴,国家发展以扩大内需为目的的新型基础设施建设,也将促进对网络安全建设的巨大需求。同时,个人隐私和信息泄露事件频发,也推动各国通过立法加强个人信息保护工作。企业面临的隐私保护合规压力不断增加,企业需要努力适应新的、更为严苛的数据隐私法规,这将有力地推动网络安全产业的快速发展。

市场空间层面,我国网络安全市场增长潜力巨大,重要行业客户的安全预算投入持续增加。2021年3月,国家发布《“十四五”规划和2035年远景目标纲要》,安全理念贯穿始终。规划中专门提出全面加强网络安全保障体系和能力建设,把网络安全与人工智能、大数据、区块链、云计算共同列为5大新兴数字产业,明确要求培育壮大,加快推动。2021年7月,工信部印发《网络安全产业高质量发展三年行动计划(2021-2023年)》征求意见稿,到2023年,我国网络安全产业规模超过2500亿元,电信等重点行业网络安全投入占信息化投入比例不低于10%。将培养一批面向车联网、工业互联网等新赛道的“专精特新”中小企业。随着车联网等新兴产业的兴起,我国的网络安全产业面临更大的机遇。

二、行业客户需求发生重大变化,取得先发优势并建立技术壁垒的企业将成为最大受益者。

从行业客户需求变化而言,客户的安全需求已从传统的形式化合规到实战化效果合法转变。全行业客户的数字化、智能化、云化转型已开展如火如荼,“互联网+”、“智能+”、“5G战略”等,推动大数据、云计算、工业互联网、物联网广泛应用,信息系统的安全也逐步改变之前围墙式、补丁式、形式合规式的业态,网络安全场景进入多元化发展期。在技术发展方面,暴增的新应用、新场景需要网络安全的新技术、新场景,促进网络安全技术进入升级换代核心期。

在当前的转折关键期,传统碎片化防护方式虽然还在发挥合规作用,但面对已经模糊的网络边界、面对难以计数的接入终端,面对无处不在的攻击面,已经无法解决新技术、新场景和新业态下的安全问题。针对愈发复杂的攻防性的网络安全问题,需要建立实战化、协同联动的纵深防御体系。只有掌握基于大数据能力下的新一代网络安全技术,拥有高效全面的应急响应能力、更强的实战化效果的安全厂商,才能给客户交付具备阻断网络安全威胁的防御方案,从而获得更多的市场商机。因此,能够满足行业客户新需求并取得先发优势、已建立技术壁垒的网络安全企业将成为未来网安市场的最大受益者。

三、实战攻防演习的监管效果日益突现,有力推动行业客户向实战化、体系化的建设方向的转变。

随着政企数字化转型的深入开展,网络攻击者的目标系统逐步转向核心业务数据和承载核心数据的业务应用。攻击者的角色也从普通的个人网络犯罪,到有组织的攻击甚至有境外背景的国家级对抗。攻击工具的武器化、攻击手段的战术化,均对政企用户的网络安全防御提出了更高要求。

为此,公安部提出“三化六防”新思想,以“实战化、体系化、常态化”为安全监管新理念,以“动态防御、主动防御、纵深防御、精准防护、整体防护、联防联控”为新举措,构建国家网络安全综合防控系统,深入推进等保和关保的积极实践。在此背景下,国家主管部门主导的国家级网络安全实战攻防演习中,参与演习的行业更加广泛,参与演习的主体数量显著增加。实战攻防演习成为政企用户网络安全保护的常态化工作,也成为政企用户检验网络安全防御体系有效性、全面提升网络安全综合防护能力的重要手段,有效地推动了政企用户增加对网络安全实战化、体系化及安全运行能力的建设投入。

四、行业技术门槛较高、高端人才极其稀缺,研发效率需要创新思路提升。

网络安全行业属于技术密集型行业,对产品研发和技术创新要求较高。一方面,网络安全技术和产品的创新能力是推动企业取得竞争优势的关键因素;另一方面,不同行业、不同政企用户对网络安全产品的技术需求也不尽相同,网络安全企业只有在充分了解用户需求的基础上,才能研发出匹配用户真实需求的产品和解决方案。此外,网络攻击和防御技术在对抗过程中会形成海量数据与知识库,如威胁情报数据库、漏洞库、病毒库等,这些知识库都需要专门的技术研究团队和产品应用团队长时间积累才能获得。

网络安全行业属于智力密集型行业,是一个高端人才极其稀缺的行业。目前国内的网络安全高端人才主要集中于国内外一些大的安全厂商以及研究机构,数量稀少,聘用成本较高且他们普遍与原单位签署了保密和竞业禁止协议,这使得市场新进入者短期内难以获得一批了解市场需求、掌握核心技术的人才团队,无法突破研发领域中的技术壁垒,从而难以形成自身的技术或差异化优势。

网络安全行业具备大量新场景、新技术需求,需要不断更新迭代新产品,传统依靠“堆人”的研发模式已经无法满足面对不断膨胀的市场新场景安全需求,网络安全创新型厂商需要通过打造“研发平台”级能力来提升中长期的研发效率降低研发成本,满足新市场新产品的快速更新迭代及低成本投入的企业发展需求;通过持续打造以“平台+工具+数据”为核心的技术研发模式,中长期降低网络安全行业对人才的依赖,增强公司核心竞争力,最终实现“降本增效”的目标,公司坚信“平台+工具+数据”的技术研发模式将助力公司未来会获得可持续性高质量增长。

五、公司核心技术能力受国内外权威机构认可、公司核心技术能力受国内外权威机构认可

公司具有领先的安全攻防与对抗技术、终端安全防御技术、大数据与安全智能检测技术、安全运营与应急响应技术,在终端安全、安全管理、安全服务、云安全、威胁情报、态势感知领域市场占有率及技术先进性排名持续领先。

2021年1月,国际权威咨询机构Forrester发布《Now Tech: External Threat Intelligence Services,Q4 2020》报告,详细盘点了全球主要威胁情报供应商(包括CrowdStrike、IBM、FireEye等),并对技术买家做出了建议。奇安信凭借海量的威胁情报样本、精准的威胁情报检测能力和强大的APT组织追踪能力,成为少数入围该报告的中国厂商之一,再次证明了奇安信威胁情报在国内的领跑地位。

2021年3月,在知识产权产业媒体IPRdaily与incoPat创新指数研究中心联合发布“科创板225家上市企业有效发明专利排行榜”中,公司以中国有效发明专利数473件、全球发明专利数量1299件位列榜单第五。作为该专利排行榜前十名中,唯一一家信息传输、软件和信息技术服务业企业,也是唯一一家网络安全企业,公司一直坚持“强研发”战略,其重视研发程度在行业内有目共睹。

2021年5月,由中国网络安全产业联盟发布的“2021年CCIA中国网安产业竞争力50强”(简称“CCIA50强”)中,奇安信被评为行业领导者企业并位居50强榜首。本次评价指标采用多维度综合评价法,对我国网络安全行业领军企业的发展状况进行综合研究,从产业视角和商业视角出发,对企业竞争力和资源力的各个维度进行了量化评估,得出50强排名。

报告期内,公司行业市场地位领先,多项新赛道产品市占率第一:

获得年份	项目	排名	来源
2021	中国安全资源池市场份额(2020全年)	1	IDC
	IT安全咨询服务厂商市场份额(2021H1)	1	IDC
	托管安全服务市场份额(2021H1)	1	IDC
	中国终端安全软件市场份额(2021H1)	1	IDC
	中国安全分析和情报市场份额(2021H1)	1	IDC
	中国政府行业IT安全软件市场份额报告(2020年全年)	1	IDC
	中国统一威胁管理(UTM)硬件市场份额(2021年全年)	3	IDC
	中国安全内容管理硬件市场份额(2021年全年)	2	IDC
	中国网络信息安全市场销售额(2020全年)	1	赛迪
	终端安全市场份额(2020全年)	1	赛迪
	安全服务市场份额(2020全年)	1	赛迪
	2020年中国云安全市场品牌TOP10排名(2020全年)	1	赛迪
	2020年中国云计算安全市场品牌结构(不含服务)(2020全年)	1	赛迪
	安全管理平台市场份额(2020全年)	2	赛迪
	Web安全市场份额(2020全年)	2	赛迪
	UTM市场份额(2020全年)	2	赛迪

报告期内,公司核心产品/创新方案上榜以下第三方机构报告:

获得年份	报告名称	品类	来源
2020	Magic Quadrant for Secure Web Gateways	SWG	Gartner
	Hype Cycle for ICT in China, 2020	云安全	Gartner
	Now Tech: Enterprise Firewalls, Q1 2020	UTM	Forrester
	Now Tech: Managed Security Services In Asia/Pacific, Q4 2020	MSS	Forrester
	Now Tech: External Threat Intelligence Services, Q4 2020	威胁情报	Forrester
	新冠疫情下,IT安全提供商如何保障企业业务稳定运行	数据安全	IDC
	CIO视角——中国智慧城市安全运营中心建设应用实践	智慧城市安全运营中心	IDC
	2020网络安全态势感知应用指南	NGSOC/监管态势感知	安全牛
2021	Market Guide for Cloud Workload Protection Platforms	云安全	Gartner
	Hype Cycle for ICT in China, 2021	云安全	Gartner
	Market Guide for Security Threat Intelligence Products and Services	威胁情报	Gartner
	New Tech: Zero Trust Network Access, Q2 2021	零信任	Forrester
	Now Tech: External Threat Intelligence Services, Q4 2020	威胁情报	Forrester
	Now Tech:Cybersecurity Consulting Services In Asia Pacific,Q3 2021	安全咨询服务	Forrester
	Now Tech Network Analysis And Visibility (NAV), Q4 2021 - Courtesy Preview	天眼	Forrester
	《IDC MarketScape中国态势感知解决方案市场2021,厂商评估》	态势感知	IDC
	《IDC MarketScape中国托管安全服务市场厂商评估,2021》	托管安全服务	IDC
	IDC PeerScape 零信任市场研究	零信任	IDC
	IDC Perspective:中国数据安全市场研究	数据安全	IDC
	IDC:中国智慧城市安全运营中心市场洞察	安全运营中心	IDC
	疫情之下政企机构互联网访问风险报告	上网行为管理	安全牛
	现代企业零信任安全构建应用指南研究报告	零信任	安全牛
	私有云环境安全防护能力构建研究报告	云安全	安全牛
	企业高级威胁防护能力构建指南	天眼	安全牛
	扩展威胁检测与响应(XDR)应用指南	扩展威胁检测与响应(XDR)	安全牛
	2020中国安全运营中心调研分析报告	安全运营中心	赛迪
	威胁情报市场指南	威胁情报	数世咨询
	XDR能力指南	EDR	数世咨询

此外,报告期内,公司荣获以下第三方机构奖项:

获得年份	奖项名称	奖项授予	来源
2020	中国网络安全企业100强	奇安信集团	安全牛
	中国网络安全能力100强-领军者	奇安信集团	数世咨询
	中国十大网络安全企业	奇安信集团	等级保护测评
	中国威胁检测与响应市场领导奖	奇安信集团	沙利文
	安全服务企业服务奖	奇安信集团	艾瑞咨询
	中国十大网络安全明星产品	奇安信网神新一代安全感知系统	等级保护测评
2021	《中国网络安全企业百强榜》	奇安信集团	安全牛
	《中国网络安全百强报告(2021)》	奇安信集团	数世咨询
	中国安全编排自动化与响应(SOAR)市场领导奖	SOAR	Frost&Sullivan
	中国网络安全APT检测市场顶级供应商名单	天眼	数说安全
	2021年度中国最强“先进计算”网络安全企业	奇安信集团	赛迪
	2021中国金融数字化转型先锋企业TOP50	奇安信集团	赛迪

3. 报告期内新技术、新产业、新业态、新模式的发展情况和未来发展趋势

回顾2021年,世界主要国家网络空间政治和军事领域力量继续保持增长态势,具有国家背景的黑客组织得到快速发展,网络空间主权的保障能力愈发重要,网络空间规则主导权和话语权争夺更加激烈。面对网络空间竞争的持续性对抗状态,以及俄乌战争中网络战的至关重要的作用,我国进一步增强网络防御手段、优化装备建设、研发自主技术已迫在眉睫。面对大国之间日益严峻的网空对抗形势,面对“新冠”疫情后的经济重建、面对“十四五”规划及新基建的快速推进,网络安全在维护国家安全、支撑产业转型、促进社会发展、保障公众利益等方面的重要作用愈加凸显。党的十九届五中全会明确了我国“十四五”期间发展的战略任务和2035年远景目标,强调要统筹发展和安全,全面加强网络安全保障体系和能力建设,网络安全已成为中国数字经济发展的底板。

从维护国家安全看,网络空间正在成为大国竞争博弈的新战场,极限施压、技术脱钩、技术民族主义等趋势对于信息技术产业链、供应链的负面影响上升,网络空间的地缘政治属性日益显现,未来万物互联的智慧社会对于网络安全防御技术能力的综合性、及时性的要求也将更高。

从支撑产业数字化转型看,产业转型升级引导网络互联互通,实现跨行业跨领域连接和海量数据采集汇聚,同时网络威胁也能直达生产一线,有效应对工业信息安全风险已经成为支撑产业转型升级的重要保障,亟需加强网络安全技术研发的前瞻性布局。

从维护社会稳定看,“新冠”疫情加速了信息化手段在城市建设和政务服务中的推广,城市治理和公共服务的泛在化、融合化、智能化水平日益提升。可以预见,各项城市公共服务和电子政务服务对于网络安全防护的需求与日俱增,构建体系化安全保障能力是必然趋势。

从保障人民利益看,“新冠”疫情期间,用户个人信息泄露和非法利用等风险正在增加,APP越权收集个人信息,个人隐私数据被暗网贩卖等各类网络违法犯罪行为层出不穷,数据安全与隐私保护领域需要全新的数据安全与隐私保护的创新型安全方案。

当前复杂又严峻的网络安全形势,加速了网络安全新技术、新理念、新业态和新模式向落地实践的转化,具体而言:

(1)内生安全框架从顶层视角构建动态综合防御体系。新基建带来复杂的应用场景,对安全防护提出更高要求,内生安全框架应运而生,从“甲方视角、信息化视角、网络安全顶层视角”出发,构建了适应不同业务场景的网络安全整体防御能力分析模型,设计了复杂异构环境下的协同联动机制,形成了全生命周期的一体化安全体系。

(2)数据安全与隐私保护场景亟需技术突破。用户信息、隐私与数据保护作为互联网治理体系的重要组成部分,也是构建良好互联网秩序的重中之重,随着大数据技术的发展,数据的挖掘、收集、整合和交易越来越普遍便利,大数据开发利用中的信息安全问题凸显。在“数据不动程序动,数据可用不可见”技术理念的驱动下,新型的数据安全产品在数据安全和隐私保护方面将采用创新性的数据沙箱和安全分离学习技术,在数据需求方部署隐私保护的前提下,对多个数据源的全量数据进行充分的分析和挖掘,数据分析师只能带走不含敏感数据的分析模型文件和分析结果。

(3)零信任理念融入身份安全场景。大数据、物联网、云计算等技术的应用改变了传统身份管理和使用模式,传统身份管理无法满足数字化身份管理需求,疫情期间远程访问激增,身份安全风险尤为突出。零信任身份安全能力侧重于解决行业客户的大数据访问与身份安全问题,立足于信息化和网络安全双基础设施的定位,构建基于属性的身份管理与访问控制体系,全面纳管数字化身份,保障业务安全持续稳定运营。

(4)车联网的网络安全场景将成为客户关注的重要领域。随着5G的加速落地,智能驾驶技术的不断成熟,车联网已经成为未来智慧交通的重要应用场景,同时其带来的网络安全问题引起广泛关注,自动驾驶性能提升带来软件代码的激增,软件缺陷中隐含大量可能被利用的漏洞,这些程序漏洞可能导致软件系统的完整性受损。车联网安全防护需要结合车联网业务场景,采用多种防护技术协同联动,通过实时感知、及时反馈的安全防护方案,为自动驾驶落地提供安全保障。

(5)工业控制系统的网络安全防护成为重要方向。工业控制系统的网络安全防护与互联网有很大区别,很多联网工业设备设计之初未考虑到网络安全设计,而工业生产的可靠性、连续性要求较高,导致针对特定工业控制设备的定期更新升级通常很困难。随着工业互联网加快应用,未来主要的安全技术发展方向包括:威胁情报通过构建攻击知识库,使得针对网络威胁的响应更快;态势感知技术面向运营技术,对各种工控数据进行全面深入的安全智能分析;纵深防御通过设置多层重叠的安全防护系统,加强整体安全能力。

(6)实战化安全运行能力建设成为客户建设的重要领域。“实战化安全运行能力建设”是立足于业务架构衍生出安全架构的组织体系建设解决方案。通过识别业务架构中支撑“生产运行”的业务驱动力、组织构成和组织行为,设计对应“安全运行”的组织建设,最终实现“生产运行”与“安全运行”的同步运行。

(7)攻防演习推动安全产品向实战化能力方向演进。为了提升国家及相关重点单位的网络安全防护水平,实战攻防演习成为了一种常态化的重要手段,通常以实际运行的信息系统作为演习目标,通过有监督的攻防对抗,最大限度地模拟真实的网络攻击,以检验信息系统的安全性和运行保障的有效性,进而推动了网络安全产品从功能趋同向防护效果差异化转变。因此,以“攻防”视角做安全的公司开始关注打造更多具备主动防御能力的产品及实战化防护效果的安全方案落地。

3 公司主要会计数据和财务指标

3.1 近3年的主要会计数据和财务指标

单位:元 币种:人民币

	2021年	2020年	本年比上年增减(%)	2019年
总资产	13,482,919,296.32	12,424,319,146.93	8.52	7,154,897,102.78
归属于上市公司股东的净资产	9,896,102,939.90	10,007,666,179.88	-1.11	5,022,490,716.75
营业收入	5,809,075,572.53	4,161,174,135.75	39.60	3,154,129,242.79
扣除与主营业务无关的业务收入和不具备商业实质的收入后的营业收入	5,781,087,273.21	4,153,504,586.22	39.19	/
归属于上市公司股东的净利润	-554,749,572.44	-334,366,055.61	不适用	-494,944,698.61
归属于上市公司股东的扣除非经常性损益的净利润	-788,162,456.44	-539,288,446.84	不适用	-688,063,342.82
经营活动产生的现金流量净额	-1,301,961,129.80	-688,556,343.32	不适用	-1,113,929,154.20
加权平均净资产收益率(%)	-5.63	-4.71	减少0.92个百分点	-12.11
基本每股收益(元/股)	-0.82	-0.54	51.85	-0.90
稀释每股收益(元/股)	-0.82	-0.54	51.85	-0.90
研发投入占营业收入的比例(%)	30.10	29.51	增加0.59个百分点	33.20

3.2 报告期分季度的主要会计数据

单位:元 币种:人民币

	第一季度(1-3月份)	第二季度(4-6月份)	第三季度(7-9月份)	第四季度(10-12月份)
营业收入	456,181,128.16	999,340,510.52	1,218,928,251.49	3,134,625,682.36
归属于上市公司股东的净利润	-536,681,476.70	-285,306,481.69	-234,935,221.06	602,172,617.00
归属于上市公司股东的扣除非经常性损益后的净利润	-553,356,040.36	-416,169,456.90	-316,198,735.89	497,561,776.72
经营活动产生的现金流量净额	-638,413,497.11	-630,051,639.23	-402,679,528.89	369,183,535.43

季度数据与已披露定期报告数据差异说明

□适用 √不适用

4 股东情况

4.1 普通股股东总数、表决权恢复的优先股股东总数和持有特别表决权股份的股东总数及前10名股东情况

单位:股

截至报告期末普通股股东总数(户)	16,854
年度报告披露日前上一月末的普通股股东总数(户)	19,290
截至报告期末表决权恢复的优先股股东总数(户)	0
年度报告披露日前上一月末表决权恢复的优先股股东总数(户)	0
截至报告期末持有特别表决权股份的股东总数(户)	0
年度报告披露日前上一月末持有特别表决权股份的股东总数(户)	0

前十名股东持股情况

(下转B551版)

证券代码:688561　　证券简称:奇安信

奇安信科技集团股份有限公司

【2022】第一季度报告

本公司董事会及全体董事保证本公告内容不存在任何虚假记载、误导性陈述或者重大遗漏,并对其内容的真实性、准确性和完整性依法承担法律责任。

重要内容提示

公司董事会、监事会及董事、监事、高级管理人员保证季度报告内容的真实、准确、完整,不存在虚假记载、误导性陈述或重大遗漏,并承担个别和连带的法律责任。

公司负责人、主管会计工作负责人及会计机构负责人(会计主管人员)保证季度报告中财务报表信息的真实、准确、完整。

第一季度财务报表是否经审计

□是 √否

一、主要财务数据

(一)主要会计数据和财务指标

单位:元 币种:人民币

项目	本报告期		本报告期比上年同期增减变动幅度(%)
营业收入	669,277,140.24		44.52
归属于上市公司股东的净利润	-480,816,938.06		不适用
归属于上市公司股东的扣除非经常性损益的净利润	-604,585,988.60		不适用
经营活动产生的现金流量净额	-989,153,562.34		不适用
基本每股收益(元/股)	-0.70		不适用
稀释每股收益(元/股)	-0.70		不适用
加权平均净资产收益率(%)	-4.88		不适用
研发投入合计	464,105,243.52		26.97
研发投入占营业收入的比例(%)	70.40		减少9.73个百分点
	本报告期末	上年度末	本报告期末比上年度末增减变动幅度(%)
总资产	12,933,359,818.13	13,482,919,296.32	-4.08
归属于上市公司股东的所有者权益	9,283,254,060.14	9,896,102,939.90	-5.18

注:“本报告期”指本季度初至本季度末3个月期间,下同。

(二)非经常性损益项目和金额

单位:元 币种:人民币

项目	本期金额	说明
非流动资产处置损益	136,137,500.18	
越权审批,或无正式批准文件,或偶发性的税收返还、减免		
计入当期损益的政府补助,但与公司正常经营业务密切相关,符合国家政策规定、按照一定标准定额或定量持续享受的政府补助除外	25,036,856.47	
计入当期损益的对非金融企业收取的资金占用费		
企业取得子公司、联营企业及合营企业的投资成本小于取得投资时应享有被投资单位可辨认净资产公允价值产生的收益		
非货币性资产交换损益		
委托他人投资或管理资产的损益		
因不可抗力因素,如遭受自然灾害而计提的各项资产减值准备		
债务重组损益		
企业重组费用,如安置职工的支出、整合费用等		
交易价格显失公允的交易产生的超过公允价值部分的损益		
同一控制下企业合并产生的子公司期初至合并日的当期净损益		
与公司正常经营业务无关的或有事项产生的损益		
除同公司正常经营业务相关的有效期内套保业务外,持有交易性金融资产、衍生金融资产、交易性金融负债、衍生金融负债产生的公允价值变动损益,以及处置交易性金融资产、衍生金融资产、交易性金融负债、衍生金融负债和其他债权投资取得的投资收益		
单独进行减值测试的应收款项、合同资产减值准备转回		
对外委托贷款取得的损益		
采用公允价值模式进行后续计量的投资性房地产公允价值变动产生的损益		
根据税收、会计等法律、法规的要求对当期损益进行一次性调整对当期损益的影响		
受托经营取得的托管费收入		
除上述各项之外的其他营业外收入和