

滴滴催化网安政策升级，政企安全投入有望大幅提升

证券分析师：熊莉

xiongli1@guosen.com.cn

证券投资咨询执业资格证书编码：S0980519030002

证券分析师：库宏焱 021-60875168

kuhongyao@guosen.com.cn

证券投资咨询执业资格证书编码：S0980520010001

事项：

“滴滴事件”从2021年7月2日至7月10日持续发酵。滴滴由于“严重违法违规收集使用个人信息问题”，旗下全部app被国家网信办要求下架，且当前正在进行网络安全审查。同时，美股上市不久的BOSS直聘、满帮集团也同样被启动网络安全审查。受此影响，计划赴美上市的Keep、喜马拉雅、零氪科技也纷纷暂停IPO。而政策层面，7月10日，《网络安全审查办法》修订草案开始征求意见，明确提出“掌握超过100万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查”。结合当前《数据安全法》等密集网络安全政策出台，上海市经济和信息化委员会软件和信息服务业处处长裘薇表示，将在即将发布的一些列政策中，进一步明确政府和公共企事业单位在网络安全上的投入比例不低于10%。

国信计算机观点：

- 1) **“滴滴事件”验证当前我国对网络安全重视程度空前，数据成为核心生产要素。**2021年开始，移动app违规收集数据频出。在“十四五”规划纲要草案中，首次将“数据”作为“生产要素”写入其中；草案明确要建立健全数据要素市场，加快完善“数据生产要素市场化”配套法律制度。
- 2) **《网络安全审查办法》征求意见再升级，网安政策密集出台。**对于我国交通关键基础设施运营者之一滴滴，《网络安全审查办法》是重要抓手。该办法已经于2020年6月1日正式实施，简单来说，就是“关键单位”采购IT产品时，必须符合“安全审核”，尤其是关键基础设施行业。今年7月10日，《网络安全审查办法》修订并征求意见，强调掌握超过100万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。同时，《数据安全法》于2021年9月1日正式实施，包括《个人信息安全保护法》等，一系列政策密集出台。
- 3) **网络安全占IT投入比有望在政府、事业单位率先达到10%，催化数倍市场空间。**根据2021年7月9日上海市经济和信息化委员会软件和信息服务业处处长的发言，未来政策中，有望明确政府和公共企事业单位在网络安全上的投入比例不低于10%。而当前，我国网络安全占IT投入比仍不到3%，仍低于全球平均水平，而美国联邦政府信息安全占IT投入比2021财年达到20%。政府是我国安全市场最大下游，占比约24%；安全投入比的提升，至少在政府领域带来一倍以上的市场空间，新增市场至少在百亿元以上。
- 4) **我国网络安全产业持续恢复，隐私和数据安全等新兴领域亟待关注。**疫情后，网络安全厂商营收增速持续恢复。从2020Q3开始到现在，全行业9家主要厂商已经进行了10次股权激励；叠加信创和常态化的攻防演习，网络安全行业重回高增长成为产业一致预期。结合当前“滴滴事件”催化，隐私和数据安全成为新的建设方向，奇安信隐私卫士、数据交易沙箱；安恒信息数据安全岛，均已走在行业前列。

重点关注网络安全板块。网络安全建设理论上没有止境，直接取决于预算投入，新兴安全领域仍有广泛建设空间。未来我国对各类IT系统的网络、数据等各类信息安全审查和投入有望实现质的提升。基于此调高行业评级，重点关注奇安信和安恒信息，以及启明星辰、天融信、绿盟科技、山石网科、深信服。



评论:

■ 滴滴事件不断发酵，网络安全审查程度空前

“滴滴”引发网络安全审查。2021年7月2日晚，国家网信办官网发布公告称，为防范国家数据安全风险，维护国家安全，按照《网络安全审查办法》，对“滴滴出行”实施网络安全审查，首先暂停了“滴滴出行”新用户注册。7月4日晚，经检测核实，“滴滴出行”App存在严重违法违规收集使用个人信息问题。目前各应用商店已下架“滴滴出行”App。7月9日晚，同样因为“严重违法违规收集使用个人信息问题”，滴滴旗下另外25款APP也被国家网信办要求下架。在“滴滴事件”期间，美股上市不久的BOSS直聘、满帮集团也同样被启动网络安全审查；而计划赴美上市的Keep、喜马拉雅、零氪科技也纷纷暂停IPO。

数据成为最重要生产要素之一，网络安全审查严格程度空前。在“十四五”规划纲要草案中，首次将“数据”作为“生产要素”写入其中。草案明确要建立健全数据要素市场，加快完善“数据生产要素市场化”配套法律制度。因此，当前对数据安全重视程度空前，尤其对于我国关键基础设施运营者，和其数据的跨境，因此《网络安全审查办法》成为重要抓手。根据官方报道，“滴滴”存在“严重违法违规收集使用个人信息问题”，而其在美国迅速上市，涉及了“国家安全”问题。该事件引发了广泛的社会影响，有望成为我国网络安全审查和建设的重要转折点，未来对各类IT系统的网络、数据等各类信息安全审查和投入有望实现质的提升。

表 1: 滴滴事件梳理

时间	事项	涉及公司
7月2日	网信办宣布对“滴滴出行”App实施网络安全审查，称“为配合网络安全审查工作，防范风险扩大，审查期间‘滴滴出行’停止新用户注册”。	滴滴
7月4日	网信办要求各应用商店下架“滴滴出行”App，通报，称“滴滴出行”App“存在严重违法违规收集使用个人信息问题”。	滴滴
7月5日	网信办宣布对在线招聘公司BOSS直聘、两家货运调度平台运满满和货车帮实施审查，审查期间以上平台停止新用户注册。注：运满满和货车帮于2017年合并为满帮集团(Full Truck Alliance)。	BOSS直聘、运满满、货车帮
7月7日	微信、支付宝无法搜索“滴滴出行”小程序，“滴滴出行”也从微信支付出行服务栏内消失。	滴滴、微信、支付宝
7月8日	健身软件Keep、播客平台喜马拉雅、阿里系医疗数据公司零氪科技(LinkDoc Technology)等取消赴美IPO计划	Keep、喜马拉雅、零氪科技
7月9日	网信办要求各网站、平台下架“滴滴企业版”等25款App，称25款App存在“严重违法违规”，各网站、平台均不得为这25款App提供访问与下载服务。	滴滴

资料来源：新浪财经，国信证券经济研究所整理

2021年上半年移动app整治同样密集。2019年关于app治理方面的政策不断出台，2021年开始进入密集整治期。根据工业和信息化部数据，截至6月21日，APP侵害用户权益专项整治行动共检查117万款APP，对4002款违规APP提出了整改要求，公开通报1248款整改不到位的APP，组织下架329款拒不整改的APP。包括滴滴在内，多数被整改的知名app应用，问题均是出在违规收集个人信息上。因此，各类《网络安全审查办法》、《数据安全法》、《个人信息保护法》等政策陆续落地，不断推动全社会信息安全建设。

表 2: APP治理事件梳理

时间	事项
2019年1月25日	中央网信办、工信部、公安部、市场监管总局四部门联合发布《关于开展App违法违规收集使用个人信息专项治理的公告》(以下简称《公告》)，决定自2019年1月至12月，在全国范围组织开展App违法违规收集使用个人信息专项治理
2019年5月27日	百款常用App申请收集使用个人信息权限情况公布
2019年12月30日	中央网信办、工信部、公安部、市场监管总局四部门联合印发《App违法违规收集使用个人信息行为认定方法》，《方法》提出，征得用户同意前就开始收集个人信息或打开可收集个人信息的权限、实际收集的个人信息或打开的可收集个人信息权限超出用户授权范围等行为可被认定为“未经用户同意收集使用个人信息”。
2021年3月22日	国家互联网信息办公室等四部门联合印发《常见类型移动互联网应用程序必要个人信息范围规定》，
2021年5月1日	关于输入法等33款App违法违规收集使用个人信息情况的通报
2021年5月15日	关于腾讯手机管家等84款App违法违规收集使用个人信息情况的通报
2021年5月21日	关于抖音等105款App违法违规收集使用个人信息情况的通报
2021年6月11日	国家网信办通报Keep等129款App违法违规收集使用个人信息的情况

资料来源：国信证券经济研究所整理



■ 《网络安全审查办法》征求意见再升级，网安政策密集出台

“滴滴”触发的《网络安全审查办法》，**关键基础设施是重点**。《网络安全审查办法》由国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、国家安全部、财政部、商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、国家保密局、国家密码管理局等 12 个部门联合发布，已于 2020 年 6 月 1 日正式实施。该《办法》重点强调了“关键信息基础设施”的保护，主要依据《网络安全法》第三十五条规定：“关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查”。简单来说，就是“关键单位”采购 IT 产品时，必须符合“安全审核”。当前主要涉及电信、广播电视、能源、金融、公路水路运输、铁路、民航、邮政、水利、应急管理、卫生健康、社会保障、国防科技工业等关键行业。显然，“滴滴”作为交通行业重要运营者，也需要网络安全审查。

《网络安全审查办法》于 7 月 10 日征求意见，**监管要求再升级**。以滴滴为代表的互联网公司，在境外上市较多。本次《网络安全审查办法（修订草案征求意见稿）》强调，**掌握超过 100 万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查**。“滴滴事件”后，该法律迅速升级，进一步扩大的覆盖范围。

表 3: 《网络安全审查办法》主要内容

	内容	说明
目的	关键信息基础设施供应链安全	维护国家网络安全
适用范围	关键信息基础设施运营者（以下简称运营者）采购网络产品和服务，影响或可能影响国家安全的	网络产品和服务主要指核心网络设备、高性能计算机和服务器、大容量存储设备、大型数据库和应用软件、网络安全设备、云计算服务等
主管机构	网络安全审查办公室；具体工作委托中国网络安全审查技术与认证中心承担	设在国家互联网信息办公室，负责制定网络安全审查相关制度规范，组织网络安全审查
运营者事先预判	应当预判该产品投入使用后可能带来的国家安全风险	如有影响，则需申报审查
获取供应商合同承诺	运营者应通过采购文件、协议等要求产品和服务提供者配合网络审查	包括承诺不利用提供产品和服务的便利条件非法获取用户数据、非法控制和操纵用户设备，无正当理由不中断产品供应或必要的技术支持服务等

资料来源：《网络安全审查办法》，国信证券经济研究所整理

网安法律密集出台，数据安全法将于 2021 年 9 月 1 日正式实施。《数据安全法》是数据领域的基础性法律，已于 2021 年 6 月 10 日表决通过，将于 2021 年 9 月 1 日起正式施行。《数据安全法》将建立数据分类分级保护制度，要求各个行业明确自身的监管职责。同时，对数据“跨境流动”提出明确监管要求，规定了数据安全审查、数据出口管制、重要数据出境管理、对等反制措施等。另一方面，政府也会进一步完善政务数据的公开和共享机制。当前我国对“数据”的保护显著提升，可以预期《个人信息安全保护法》、《关键信息基础设施安全保护条例》等正式文件也会陆续出台。

表 4: 网络安全政策密集出台

日期	相关部门	名称	要点
2020.04.27	网信办、发改委、工信部、公安部、国安部等 12 个部门	《网络安全审查办法》	关键信息基础设施运营者采购网络产品和服务，影响或可能影响国家安全的，应当按照本办法进行网络安全审查。
2020.10.21	全国人大法工委	《中华人民共和国个人信息保护法(草案)》	明确生物特征、医疗健康、金融账户、种族民族等多种敏感信息，增强了违法个人信息处理行为的法律责任，最高处罚可达 5000 万元或上一年度营业额 5%
2021.03.22	网信办、工信部、公安部、市场监督管理总局	《常见类型移动互联网应用程序必要个人信息范围规定》	App 不得因为用户不同意提供非必要个人信息，而拒绝用户使用其基本功能服务。
2021.06.10	全国人大常委会	《数据安全法》	确立数据分级分类管理以及风险评估、检测预警和应急处置等数据安全各项基本制度；明确开展数据活动的组织、个人的数据安全保护义务，落实数据安全保护责任；同时加大对违法行为的处罚力度
2021.07.10	网信办	《网络安全审查办法(修订草案征求意见稿)》	掌握超过 100 万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。

资料来源：政府官网，国信证券经济研究所整理

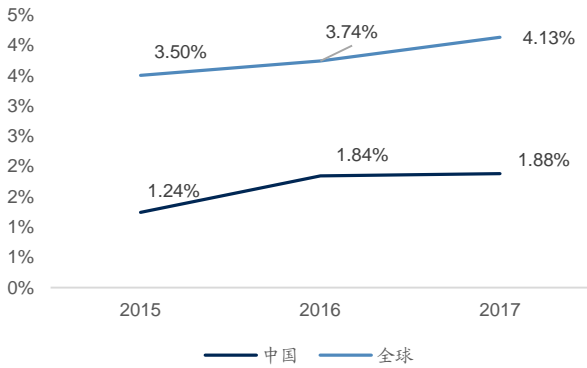
■ 滴滴事件不断发酵，网安投入比向 10% 目标进发

安全占 IT 投入逐步将以 10% 为目标，当前不到 3%。“滴滴事件”验证了网络安全政策强大的执行力，同时各类政策仍在积极制定和完善。2021 年 7 月 9 日，在上海举办的世界人工智能大会安全论坛上，上海市经济和信息化委员会软件和信息服务处处长裘薇表示，正和网信办协商，在今年发布的网络安全“十四五”规划，以及即将发布的网络安全产业的行动计划当中，进一步明确政府和公共企事业单位在网络安全上的投入比例不低于 10%。无独有偶，在 2020 年 11 月底，北京的 2020 年中国网络安全产业高峰论坛中，工信部副部长刘烈宏也说到“增加网络安全占信息系统建设投入的比重。我们希望这个比重至少要突破 5%”。



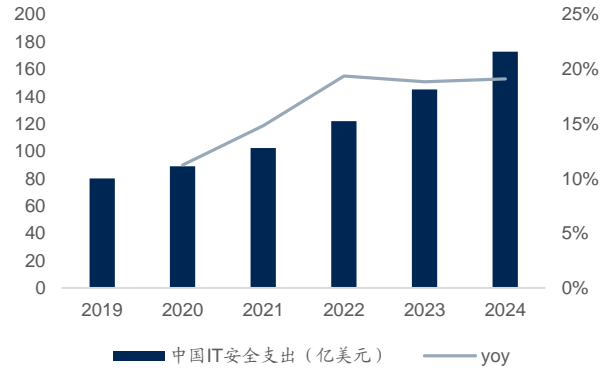
我国当前信息安全占 IT 投入比不到 3%，市场不到 600 亿。根据 IDC 数据，2017 年我国安全占 IT 投入比为 1.88%，全球平均 4.13%，仍有一倍以上差距。根据 2020 年 IDC 数据，我国 IT 市场 2.07 万亿，其中安全市场约 79 亿美金，500 多亿人民币；结合其他第三次测算也不到 600 亿人民币，因此计算下来，整体安全占 IT 投入比不到 3%。随着《网络安全法》、等保 2.0 等一系列政策推动，信息安全投入占比有望持续提升，带来数倍市场空间。

图 1：全球及中国信息安全投入占 IT 投入比



资料来源：IDC，国信证券经济研究所整理

图 2：中国 IT 安全市场支出预测（美金）

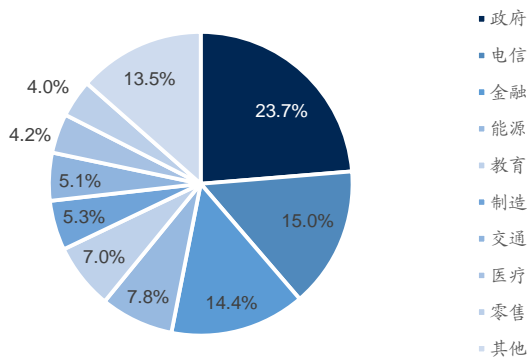


资料来源：IDC 2021，国信证券经济研究所整理

政府是网安行业最大下游，有望率先达到 10% 目标。由于政府对网络安全、IT 合规等方面的要求更为普及，因此政府一直是网络安全最大的下游市场，占比达到 23.7%。所以也可以推测我国网络安全建设中，政企、事业单位较为领先，因此安全占 IT 投入比应该高于全国平均水平，但预期也不会高于 5%。结合当前政策预期，安全占 IT 投入比，有望率先在政府、事业单位达到 10% 的目标，因此保守估计也至少有一倍以上的新增市场空间。而从企事业单位 IT 建设的角度上来看，网络安全建设是没有严格边界的，因此细分行业和产品众多。这也说明，IT 预算和安全投入最为重要，只要有足够预算，市场可以持续扩张：老产品因为新的 IT 建设正常增长，新产品可能在高要求企业中已率先应用，如零信任、数据安全分级等。因此，安全占 IT 投入比的提升，将全面带动行业快速增长。

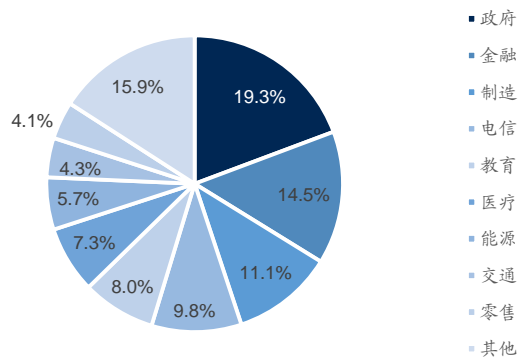
美国联邦政府 2021 财年网络安全预算占 IT 预算比值超过 20%。根据美国联邦政府公布 2021 财年预算草案，2021 财年网络安全（Cybersecurity）领域的预算有 188 亿美元（不含涉密预算），其中国防部占了 98.5 亿美元，占比超过一半；民事部门是 90 亿美元；国土安全部占了 26 亿美元；司法部占了 9.3 亿美元。按技术划分，识别、保护、检测、响应和恢复五个环节的预算都有所增长。整体上，美国联邦政府的网络安全预算占 IT 预算的比重是 20.4%，绝对金额和占比均有增加。参考美国，我国政府领域信息安全投入有望持续加大。另一方面，对比全球，我国政府之外的其他行业安全投入更低，因此政策要求可能会向其他行业覆盖。

图 3：2019 年中国网络安全市场行业划分



资料来源：Frost&Sullivan，国信证券经济研究所整理

图 4：2019 年全球网络安全市场行业划分



资料来源：Frost&Sullivan，国信证券经济研究所整理

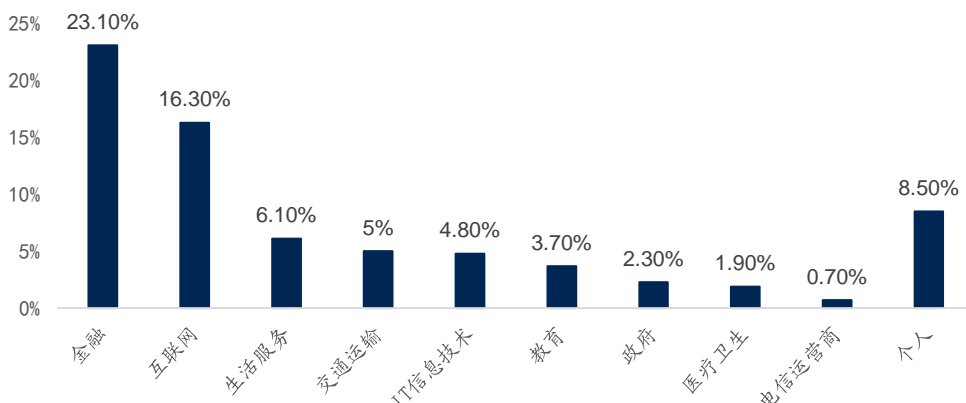
■ 数据安全、隐私保护在风口浪尖，新兴安全领域建设无止境

网络安全审查、数据安全法、加强对移动 app 信息收集监管等这一系列政策推出，安全行业又将迎来新增长点。对数据安全的强调，进一步推动信息化建设中内生安全的融入，即进入数据全生命周期的各个环节，不再只是后 IT 时



期的修修补补。数据生命周期涉及采集、传输、存储、处理、交换、销毁。当前的网络安全建设，主要仍基于传输和存储两个环节，像“交换”之类敏感环节，并未成熟，才导致数据泄露和数据黑市的存在。因此传统及新兴数据安全技术有望得到迅速应用和发展，如数据加密（叠加当前国密改造）、脱敏；数据监测（态感、UEBA）、数据审计（堡垒、水印）；隐私计算；数据容灾等，未来也能看到持续的产品化及方案落地。根据《2018年暗网非法数据交易总结》数据，暗网上数据交易涉及多个行业，其中金融行业占比最高，达到23.1%；互联网行业次之，占比为16.3%。个人信息的数据高达8.5%。灰色数据交易亟待安全技术来解决。

图 5：暗网数据交易涉及行业



资料来源：《2018年暗网非法数据交易总结》，国信证券经济研究所整理

网络安全建设无止境，PPDR 是短期目标。信息安全的范畴，从一个个独立 PC 下的杀毒软件，逐步进化到互联网时代的防火墙等设备，攻防和数通两大能力成为安全厂商的基本盘，各产品单兵作战发挥各自的价值。随着 IT 资源云化等逐步迭代，全局视角下的数据分析成为安全的必然发展方向。根据 Gartner 的 PPDR 安全模型，从最开始的堆设备防御和检测，要逐步进化到对安全事件的自动响应及预测，因此以大数据分析为代表的 UEBA 技术、以自动编排为代表的 SOAR 技术都是现代安全发展的重点细分，最终成为全局可视下的智能态势感知平台。大数据的能力将安全厂商带入新的高度，可以全面覆盖企业网的网络管理及运维。

因此，政府领域网络安全预算的提升，除了可以正常覆盖信息化建设带来的传统安全产品外，还能进一步提升在零信任、态势感知、泛终端、威胁情报、云安全等多个领域的安全建设。

图 6：安全能力逐步进化



资料来源：国信证券经济研究所整理

图 7：PPDR 模型



资料来源：Gartner，国信证券经济研究所整理

■ 信息安全行业有望持续回暖，长期成长确定无疑

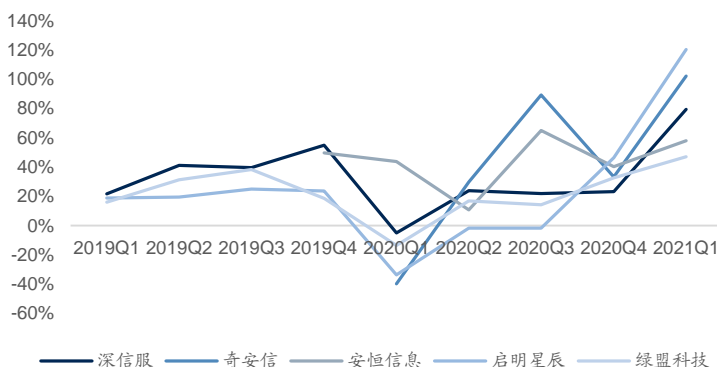
我国网络安全市场重回高增长。根据《IDC 全球网络安全支出指南，2021V1》，2021 年全球网络安全市场达到 1435 亿美元，同比增长 8.7%；2019-2024 年复合年均增长率达到 9.41%，行业仍保持稳步增长。我国行业增速显著高



于全球水平，2021年国内安全市场有望达到102.2亿美元，2024年达到172.7亿美元，2020-2024年复合增长率达到16.8%。我国当前对信息安全领域重视空前，各类政策不断完善；在疫情恢复后，2021年开始行业将呈现加速态势。

各大信息安全厂商增速回暖，行业有望重回高景气。疫情对信息安全产业负面影响较大，2020年上半年行业整体基本处于负增长状态。但是头部厂商产品布局更新，市场战略更为激进，因此二三季度开始明显恢复。头部厂商在新兴安全领域布局较深，细分增速也快于行业平均水平；20Q4和21Q1各大厂商均出现。2020年是等保2.0正式实施的第一年，信息安全在信息化建设中占比越来越高；整体上看，各大网络安全厂商均有效克服了疫情的不利影响，依然保持至少20%左右的全年营收增长，2021Q1全行业均保持较高增长。

图 8：五家网络安全厂商季度增速



资料来源：公司公告，国信证券经济研究所整理

全行业积极股权激励，捆绑核心人才看好发展。信息安全行业人才稀缺性大，各个厂商均有加大对核心技术人才的激励。从考核目标上看，均没有设置过高的目标。从激励时间来看，全行业均集中在2020Q3开始，一定程度上也认为上半年是行业发展低点，下半年开始行业进入全面回暖。在众多安全厂商中，安博通作为厂商的厂商，扮演了行业上游的角色，其2021年收入目标在2020年目标基础上增长了40%，也表明了行业对明年产业回暖的信心。

信创和攻防演习叠加，产业形成高增长共识。2021年是网络设备信创大年，以防火墙为代表的产品有望迎来替换高峰。同时，2021年重大事件较多，网络安全攻防演习投入有望进一步加大。因此，结合当前全行业股权激励，行业高增长成为产业共识。

表 5：网络安全全行业股权激励

公司	时间	业绩考核
奇安信	2020年10月30日	以19年营收为基数，20-23年收入增长率不低于25%/55%/90%/135%
深信服	2020年7月7日	以2019年营业收入为基数，20-22年营收增速不低于5%/10%/15%
安恒信息	2020年8月26日	以2019年营业收入为基数，20-23年营收增长率不低于25%/50%/75%/100%
启明星辰	2020年9月23日	以2019年营业收入为基数，20-22年营业收入增长率不低于5%/10%/15%
天融信	2020年9月9日	以2019年营业收入为基数，20-22年营业收入增长率不低于10%/20%/30%；或者20-22年净利润不低于6.5/7.5/8.5亿元(二选一)
安博通	2020年10月31日	20-22年营业收入不低于2.5/3.5/4.5亿元
山石网科	2020年12月4日	以2020年营收为基数，21-24年营收增长率不低于25%/50%/75%/100%
迪普科技	2021年3月5日	以2020年营收为基数，21-23年营收增长率不低于20%/40%/60%
绿盟科技	2021年4月23日	以2020年营收为基数，21-23年三档考核目标分别为复合20%、复合10%、复合5%营收增速
天融信	2021年5月31日	以2020年营业收入为基数，21-23年营业收入增长率不低于10%/20%/30%；或者21-23年净利润不低于7.5/8.6/10亿元(二选一)

资料来源：公司公告，国信证券经济研究所整理

■ 奇安信和安恒信息在数据安全领域发力领先

奇安信在数据和隐私安全方向走在前列。滴滴被诟病的“App存在严重违法违规收集使用个人信息问题”。2021年2月，工信部通报了2021年首批157款侵害用户权益行为APP，其中涉及违规使用个人信息、违规收集个人信息问题，占比高达86.6%。奇安信是国内为数不多具备移动安全能力的厂商，在2020年就推出隐私卫士，一款支持



安卓和苹果 IOS 两大系统移动应用隐私合规检测与分析的系统。该产品可对个人信息采集的方式(自身采集/第三方采集)、使用权限(自身使用/第三方使用)、采集频率、是否出境、是否与隐私政策描述实质符合等进行合规检测，隐私合规检测技术与能力得到工信部一致认可。

图 9: 奇安信隐私卫士



资料来源: 奇安信官网, 国信证券经济研究所整理

针对最敏感的“数据交易”环节，今年 5 月奇安信正式发布数据安全开放平台“数据交易沙箱”。数据拥有方提供数据，在“沙箱”中进行交易和计算，这样需求方只能使用而无法获取，真正实现数据隐私安全，达到“数据不动程序动”、“数据可用不可见”的安全理念。尤其是政府单位，拥有最全面的数据，如果充分利用价值难以估量；但现实往往是害怕数据泄露，而“不敢”，“不能”充分利用。早在 2015 年，贵阳大数据交易所的成立已开始探索数据的确权、交易等安全技术；按照交易所的说法，数据交易所的成交额与黑市相比只有 1%。奇安信“数据交易沙箱”是当前隐私计算技术应用、数据安全领域的代表产品，数据安全必将成为下一个高速成长的赛道。

图 10: 奇安信数据交易沙箱



资料来源: 奇安信官网, 国信证券经济研究所整理

安恒信息定增积极在新兴领域投入，其中数据安全是重点。安恒此次定增募资 13.33 亿元，总投资在 17.14 亿元。从项目布局来看，一是延伸，公司继续加强在政府、公安领域安全需求的挖掘；二是补短，公司 2019 年网络层安全产品仅占收入的 5.19%，而防火墙依然是当前最大的细分市场，2019 年占比 38%；三是创新，在前沿的车联网领域提前布局，加大安全教育市场的投入。其中数据安全岛项目投资额较大，也是公司重点发力的方向。

表 6: 安恒信息定增项目

项目名称	总投资	募集资金拟使用额
数据安全岛平台研发及产业化项目	47,633.85	40,046.62



涉网犯罪侦查打击服务平台研发及产业化项目	13,006.66	10,216.18
信创产品研发及产业化项目	62,122.22	45,870.82
网络安全云靶场及教育产业化项目	15,753.23	12,541.34
新一代智能网关产品研发及产业化项目	22,622.09	17,924.13
车联网安全研发中心建设项目	10,235.45	6,733.08
合计	171,373.50	133,332.17

资料来源：安恒信息公告，国信证券经济研究所整理

安恒信息以应用和数据安全起家，数据安全岛已获得市场认可。AiLand 数据安全岛是一个专注于保障数据安全流通的隐私计算平台，实现共享数据的所有权和使用权分离，确保原始数据的“可用不可见”、“可用不可取”。产品采用了综合应用安全计算沙箱，联邦学习，区块链，密文计算等多种数据安全技术，在赛迪“2021 IT 市场年会”中获得“新一代信息技术创新产品”奖。AiLand 数据安全岛未来有望在数据开放、挖掘、共享、交换等领域发挥价值。

图 11：安恒信息数据安全岛



资料来源：安恒信息官网，国信证券经济研究所整理

投资建议

看好整个网络安全板块，重点关注奇安信和安恒信息。随着“滴滴事件”不断发酵，以及相关政策不断加码，网络安全仍是最具景气度和确定性的成长性行业。当前我国网络安全占 IT 投入比不到 3%，政府领域有望率先提升至 10%，对于在政府领域深耕的厂商有望率先获益。奇安信在政府领域耕耘较深，尤其是常态化的网络安全攻防演习，奇安信已经成为各类政府单位的重要合作伙伴；同时，公司在新兴安全领域投入最多，如态势感知、零信任、云安全等等均处于行业领先。安恒信息在政府、公安领域发展较快，态势感知也是公司标杆产品，公司进一步在上海临港投资，打造一站式工业互联网服务云基地、数据安全岛基地、全球网络安全保险基地、长三角信创研发运营基地。另一方面，其他网络安全厂商也积极布局，如政府领域布局积累较多的启明星辰、天融信；数据安全积累较多的绿盟科技（包括亿赛通）；“3D”数据安全治理方案入选 IDC 的山石网科；云安全领域持续布局的深信服（SASE）等。因此，我们持续看好网络安全板块，重点关注奇安信和安恒信息，以及启明星辰、天融信、绿盟科技、山石网科、深信服。

风险提示

各类网络安全政策推进和执行不达预期。

市场竞争加剧，全行业盈利能力下滑。

疫情等负面影响反复，导致 IT 支出下降。



相关研究报告:

- 《国信证券-地产数字化专题—全球 3D 云设计软件龙头厂商（群核科技）》
- 《EDA 行业报告：从华大九天看国产 EDA 的“逆风而上”》
- 《国信证券-IDC 行业专题-IDC 产业链景气周期及投资框架分析》
- 《行业月报：中报业绩催化半导体板块行情》
- 《国信证券-Roblox (RBLX.N)-深度报告：元宇宙“头号玩家”、全球游戏 UGC 平台开创者》

国信证券投资评级

类别	级别	定义
股票 投资评级	买入	预计 6 个月内，股价表现优于市场指数 20%以上
	增持	预计 6 个月内，股价表现优于市场指数 10%-20%之间
	中性	预计 6 个月内，股价表现介于市场指数 $\pm 10\%$ 之间
	卖出	预计 6 个月内，股价表现弱于市场指数 10%以上
行业 投资评级	超配	预计 6 个月内，行业指数表现优于市场指数 10%以上
	中性	预计 6 个月内，行业指数表现介于市场指数 $\pm 10\%$ 之间
	低配	预计 6 个月内，行业指数表现弱于市场指数 10%以上

分析师承诺

作者保证报告所采用的数据均来自合规渠道，分析逻辑基于本人的职业理解，通过合理判断并得出结论，力求客观、公正，结论不受任何第三方的授意、影响，特此声明。

风险提示

本报告版权归国信证券股份有限公司（以下简称“我公司”）所有，仅供我公司客户使用。未经书面许可任何机构和个人不得以任何形式使用、复制或传播。任何有关本报告的摘要或节选都不代表本报告正式完整的观点，一切须以我公司向客户发布的本报告完整版本为准。本报告基于已公开的资料或信息撰写，但我公司不保证该资料及信息的完整性、准确性。本报告所载的信息、资料、建议及推测仅反映我公司于本报告公开发布当日的判断，在不同时期，我公司可能撰写并发布与本报告所载资料、建议及推测不一致的报告。我公司或关联机构可能会持有本报告中所提到的公司所发行的证券头寸并进行交易，还可能为这些公司提供或争取提供投资银行业务服务。我公司不保证本报告所含信息及资料处于最新状态；我公司将随时补充、更新和修订有关信息及资料，但不保证及时公开发布。



国信证券经济研究所

.....

深圳

深圳市罗湖区红岭中路 1012 号国信证券大厦 18 层

邮编: 518001 总机: 0755-82130833

上海

上海浦东民生路 1199 弄证大五道口广场 1 号楼 12 楼

邮编: 200135

北京

北京西城区金融大街兴盛街 6 号国信证券 9 层

邮编: 100032

