内部发行 免费赠阅

出版物准印证号：京内资准字 2122- L0058 号

SECURITY INSIDER

网安26号院

奇安信网络安全通讯 · 安全快一步

合规！冲刺！

—2022网络安全合规指南

P12

第22期
2022 年 10 月

奇安信
新一代网络安全领军者

打造新一代中国特色的安全托管服务

时刻守护您的网络安全

奇安信安全托管服务以威胁发现为基础、以分析处置为核心、以发现隐患为关键、以解决客户问题为目标，7*24小时全天候全方位守护客户网络安全。

两种模式
模式随心选择

- 直营服务模式：奇安信产品+MSS
- 合作服务模式：技术、产品、服务整体托管

多种形态
全面助力建成

- 城市运营中心
- 行业安全运营中心
- 企业安全运营中心

两化融合
帮您真正实现

- 集中服务化：统一监测、预警与通报
- 服务集中化：标准统一、质量可控、资源共享

首创“云地结合”模式

打破传统的托管仅限“云端监测”的认知开辟“云地结合”模式，云端+地端实现真正的闭环服务。

7*24h实时持续监测

“地球不爆炸，我们不放假”——7*24h持续监测，充分保障常态化运营。

安全事件响应快一步

对APT攻击、网络攻击等长效监测，提前预警，响应快一步。

安全事件处置规范化

事前检测、事中分析、事后总结，真正实现闭环，并在实战中不断加固。

专家“一对一”指导

专家通过视频一对一的方式与您“面对面”沟通指导，不仅让您了解现状，还能防患于未然。

新安全格局下，网安合规该怎么做？

党的二十大报告中 26 次提及“国家安全”，将“国家安全”提升至事关“民族复兴的根基”的高度，并从统筹发展和安全的战略高度对国家安全做出新的部署，要求“扎实推进国家安全体系和能力现代化，以新安全格局保障新发展格局”。

报告对“国家安全体系和能力现代化”，以“新安全格局”论述，体现出对未来五年乃至更长时期对于国家安全问题的统筹考量和规划。

网络安全是国家安全的重要内容。习近平总书记曾指出，没有网络安全就没有国家安全。网络安全与信息化是事关国家安全与发展的的重大战略问题。二十大报告意味着未来我们将会进一步推进包括网络安全在内的国家安全能力现代化建设，以更高水平的安全为更高质量的发展来托底。

网络安全合规是实现网络安全、保障国家安全的基础。目前我国的网络安全法律法规不断完善和丰富，2017 年 6 月实施《 中华人民共和国网络安全法 》；2019 年 12 月实施“网络安全等级保护制度 2.0 标准”；2021 年实施《 关键信息基础设施安全保护条例 》《 中华人民共和国数据安全法 》，以及《 中华人民共和国个人信息保护法 》；2022 年 9 月，《 网络安全法 》迎来首次修改，进一步压实网络安全责任、大幅提高重大网络安全事故处罚力度。

政策法规、规章条例的数量之多，政策推出的频度之密，凸显了网络安全合规的重要性和紧迫性。以《 网络安全法 》《 数据安全法 》《 个人信息保护法 》等为代表的网络空间安全法治建设，为维护国家总体安全、抵御网络空间各种不确定性因素和未知风险发挥了重要作用。

在网络安全保障方面，目前政企机构有 6 项法定合规义务需要遵守和落实，包括实施网络安全等级保护的义务、关键信息基础设施保护义务、数据安全保护义务、个人信息保护义务、违法有害信息的治理和禁止从事危害网络安全的义务等。

未来，随着我们继续推进国家安全体系和能力现代化，以及新安全格局的建设，网络安全合规建设成为数字经济时代政企机构的核心挑战和首要任务。

政企机构如何实现网络安全合规，这不是买了多少产品、投入多少人员就能一下子解决全部合规问题，既涉及对合规义务的梳理，更是持续优化合规能力的过程。

《 网安 26 号院 》第 10 期，以网络安全合规指南为主题，回顾总结 2022 年的法律法规动向，解读网络安全合规的要点和需要发展的合规能力，希望给政企用户提供一份最全面、最体系的网络安全合规实操指南。

总编辑

李建平

2022 年 10 月 1 日

CONTEN

目录

安全态势

月度专题

合规！冲刺！

—2022 网络安全合规指南 P12

网络安全合规是实现网络安全、保障国家安全的基础，我们要以更高水平的安全为发展来托底。

TS

《网安 26 号院》编辑部

主办 奇安信集团

总　　编　　辑：李建平
安全态势主编：王　彪
月度专题主编：李建平
攻防一线主编：魏开元
安全之道主编：张少波
奇安信人主编：孙丽芳
安全叨客主编：王梦琪
奇安资讯主编：陈　冲
研究报告主编：包世玉

奇安信集团　虎符智库　安全内参

索阅、投稿、建议和意见反馈，请联系奇安信集团公关部

索阅邮箱：26hao@qianxin.com
地　　址：北京市西城区西直门外南路 26 院 1 号
邮　　编：100044
联系电话：（010）13701388557
出版物准印证号：京内资准字 2122- L0058 号
印刷数量：4500 本
印刷单位：北京博海升彩色印刷有限公司
印刷日期：2022 年 10 月 26 日
发行对象：奇安信集团内部

版权所有 ©2022 奇安信集团，保留一切权利。
非经奇安信集团书面同意，任何单位和个人不得擅自摘抄、复制本资料内容的部分或全部，并不得以任何形式传播。

无担保声明
本资料内容仅供参考，均“如是”提供，除非适用法要求，奇安信集团对本资料所有内容不提供任何明示或暗示的保证，包括但不限于适销性或者适用于某一特定目的的保证。在法律允许的范围内，奇安信在任何情况下都不对因使用本资料任何内容而产生的任何特殊的、附带的、间接的、继发性的损害进行赔偿，也不对任何利润、数据、商誉或预期节约的损失进行赔偿。

内部发行　免费赠阅

事件篇

全球关基设施网络威胁突出，印度塔塔电力遭网络攻击影响部分 IT 系统，伊朗国家电视台播出画面再次被篡改，美国超级连锁医院因勒索攻击引发 IT 崩溃，俄乌冲突密集战争更导致乌克兰关基保护负责人死亡。

勒索攻击中断印刷系统，德国地方大报被迫暂停纸质版发行

据 BleepingComputer 10 月 17 日消息，德国地方报纸《海尔布隆言论报》因遭遇勒索软件攻击，印刷系统陷入瘫痪，被迫暂停纸质版发行。该报在海尔布隆地区的发行量约有 7.5 万份，目前只能通过官方网站提供查看服务。此次攻击还影响了该报母公司 Stimme Mediengruppe 媒体集团，旗下 Echo 等其他报纸的电子版均无法访问，其在当地代理发行其他主要报纸的工作也无法进行。

印度塔塔电力遭网络攻击，公司部分 IT 系统受影响

据路透 10 月 15 日消息，印度最大的综合发电公司塔塔电力在周五（14 日）晚间披露，一起针对其 IT 基础设施的网络攻击影响了部分系统运作。该公司表示，已采取措施检索和恢复系统，所有关键操作系统都在运行。为谨慎起见，塔塔电力还对员工、客户门户和接触点实施了限制访问策略和防范性检查。

深圳证监局通报：某券商 OA 系统遭攻击，影响移动办公

据证监会网站 10 月 13 日消息，深圳证监局公布了 2022 年第 5 期证券期货机构监管通信，其中通报了一起证券公司网络安全风险管理不规范的风险案例。通报称，辖区某证券公司因网络安全风险管理存在漏洞，导致公司 OA 系统遭受注入攻击影响公司移动端 OA 办公。深圳证监局核查发现，该公司渗透测试及漏洞修复机制不完备，网络安全监控方式和响应机制有待改进，安全防护策略有待加强。同时，该公司信息系统相关人员流动较大，多个重要信息系统运维主岗已离职，多个技术管理环节权限管理不严。

俄乌网络战惨烈时刻：乌克兰关基保护负责人因导弹袭击丧生

据 TheRecord 10 月 11 日消息，乌克兰国家警察局披露，因 10 日首都基辅遭受俄罗斯导弹袭击，关键基础设施保护部门负责人 Yuriy Zaskoka 丧生。乌克兰国家特别通信局还称，该局在前线关基设施工作的 4 名雇员也因此死亡。本轮导弹袭击还导致乌克兰大范围停电，进而引发互联网与移动通信中断。Cloudflare 称，10 日早上乌克兰互联网可用性较正常水平下降了 35%。

伊朗社会抗议引发国家电视台再次被篡改，播放“杀死最高领袖”画面

据 SecurityWeek 10 月 9 日消息，支持伊朗女性抗议浪潮的黑客劫持了该国国家电视台的播报，在画面中放出最高领袖阿亚图拉 · 阿里 · 哈梅内伊 (Ayatollah Ali Khamenei) 头部被十字准星瞄准并在火焰中燃烧的形象。该视频在互联网上广泛传播。尽管伊朗已经全面中断了国内互联网的连接，封锁了各大主要社交媒体平台，但该国惨烈的对抗、令人毛骨悚然的血腥镜头、攻击政要形象的视频仍然在网络上广为流传。这是今年来伊朗国家电视台第二次遭到篡改攻击。

因开发人员误公开源代码，丰田或泄露近 30 万客户信息

据南方都市报 10 月 8 日消息，丰田汽车发现，296019 名客户的电子邮件地址和客户编号可能被泄露，但客户姓名、电话号码和信用卡等敏感个人信息均未受到影响。受影响的可能是 2017 年 7 月之后用电子邮件注册丰田 T-connect 服务的客户。T-connect 是丰田的远程车载信息通信服务，车主可通过网络连接车辆。丰田调查发现，客户信息之所以被泄露，是因为开发 T-connect 网站的承包商将部分源代码上传到 GitHub 账号上，并不小心将权限设置成“公开”。丰田表示，公开源代码的操作违反了汽车制造商的处理规定。

美国超大型连锁医院因勒索攻击引发 IT 崩溃：救护车改道、电子病历失联

据 The Register 10 月 6 日消息，美国第二大非营利性医疗保健组织 CommonSpirit Health 旗下的部分机构遭遇 IT 安全问题，被迫转移救护车路线，关闭全国各地医院的电子病历系统。有消息人士称，该组织遭受的是勒索软件攻击。CommonSpirit Health 总部位于芝加哥，在全美 21 个州拥有 1000 多处设施和 140 家医院。医疗网络威胁日益猖獗，今年已有多家大型医疗机构因此停业或业务中断。

网络攻击扰乱酒店供应链！洲际酒店集团加盟商损失惨重

据华尔街日报 9 月 26 日消息，洲际酒店集团在 9 月初表示，检测到技术系统中存在未授权活动，导致预订及其他系统出现严重中断。这影响到了各特许加盟商的业务，导致愤怒的客户、收入损失乃至集体诉讼隐患持续发酵。有加盟的酒店业主估算，此次网络攻击对单家酒店造成的平均损失在 30000 到 75000 美元之间，洲际酒店集团全球约有 6000 家酒店。酒店业主们希望获得赔偿并了解事件细节，为此已向洲际酒店集团发起集体诉讼。

印度一医疗公司毫无责任心：新冠抗原检测数据公网暴露无人处理

据 HackRead 9 月 25 日消息，印度一家医疗软件提供商的Elasticsearch服务器被发现暴露在互联网上，其中存储了过去几年来往返于印度各地的众多印度及外国人的 COVID 抗原检测结果。受害者人数超过 170 万，涉及印度、美国、加拿大等多国公民，具体数据包括姓名、详细地址、电话、Aadhaar 医保编号、护照编号、基础疾病情况等敏感个人信息。研究员将暴露情况告知该公司，但一周后该公司既未回复也未处理，相关数据库仍可访问，体现了该公司极不负责任的态度。

漏洞篇

微软 Exchange Server 又爆出多个远程命令执行漏洞，官方已提供临时修复措施，但尚未发布修复补丁，建议相关用户尽快采取防护措施。

Apache Shiro 身份认证绕过漏洞安全风险通告

10 月 12 日，奇安信 CERT 监测到 Apache Shiro 身份认证绕过漏洞 (CVE-2022-40664)，当使用 RequestDispatcher 进行请求处理时，Apache Shiro 存在身份认证绕过漏洞，此漏洞影响 Shiro 1.10.0 之前的版本。鉴于该漏洞影响较大，建议客户尽快做好自查及防护。

VMware vCenter Server 远程代码执行漏洞安全风险通告

10 月 11 日，奇安信 CERT 监测到 VMware vCenter Server 远程代码执行漏洞 (CVE-2022-31680)，VMware vCenter Server 6.5 的 Platform Services Controller 功能中存在一个不安全的反序列化漏洞，拥有高权限的远程攻击者可以发送特制的 HTTP 请求来触发此漏洞，最终可导致远程代码执行。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

Fortinet FortiOS 安全漏洞情况通报

10 月 10 日，国家信息安全漏洞库（CNNVD）收到关于 Fortinet FortiOS 安全漏洞（CVE-2022-40684）情况的报送。成功利用漏洞的攻击者，可在未经身份验证的情况下获得对管理界面的访问权限，从而最终控制目标系统。Fortinet FortiOS 7.0.0 版至 7.0.6 版、7.2.0 版至 7.2.1 版、FortiProxy 7.0.0 版至 7.0.6 版、7.2.0 版本等多个版本均受此漏洞影响。目前，Fortinet 官方已发布升级补丁修复了该漏洞，建议用户及时确认产品版本，尽快采取修补措施。

微软 Exchange Server 多个安全漏洞通报

10 月 9 日，国家信息安全漏洞库（CNNVD）收到关于微软 Exchange Server 多个安全漏洞（CVE-2022-41040、CVE-2022-41082）情况的报送。经身份验证的攻击者利用服务端请求伪造漏洞，可远程访问 PowerShell，进而导致在目标系统远程代码执行。Exchange Server 多版本受漏洞影响。目前，微软官方已公告上述漏洞并提供临时修复措施，请用户及时确认是否受到漏洞影响，尽快采取修补措施。

Cobalt Strike 远程代码执行漏洞安全风险通告

9 月 21 日，奇安信 CERT 监测到 Cobalt Strike 远程代码执行漏洞，当攻击者访问 Beacon 的监听器时，可以在连接 Beacon 的 listener 时使用错误的用户名，触发 XSS，造成远程代码执行。鉴于该漏洞影响范围极大，建议客户尽快做好自查及防护。

对抗篇

国内攻防演习 9 月态势：哪些薄弱点最易被利用?

作者 奇安信安服团队

一、本月演习整体情况

2022 年 9 月，奇安信 Z-Team 团队共承接攻防演习服务 34 场，其中省级攻防演习 3 场，省级行业攻防演习 1 场，地市级攻防演习 5 场，本单位自主攻防演习 25 场。

本月攻防演习成果如下：

二、本月任务目标特点

本月攻防演习和评估任务行业比较分散，覆盖目标面比较广，涵盖了政务、金融、交通、教育、互联网企业等目标，客户存在的安全问题主要有互联网业务平台存在漏洞、业务系统敏感信息泄露、内部人员对钓鱼攻

目标系统	靶标	强隔离内网	核心业务网	网站	堡垒机	安全设备	业务系统	服务器
数量	27	46	55	87	23	108	174	781

击防范意识不足、内部网络安全防护措施缺乏、内网口令复用及弱口令普遍等。具体情况如下。

1、漏洞利用依旧是外网成功突破的主要手段

本月任务中针对多行业的不同目标网络，漏洞利用是外网成功突破的主要手段。被攻陷目标互联网侧应用漏洞以平台组件漏洞为主，如 Web 应用中 Struts2 组件漏洞、Shiro 反序列化漏洞、Apache Log4j2 远程代码执行漏洞、AMF 反序列化漏洞等，其多因外部应用及系统组件更新不及时造成，直接给目标网络带来了严重的安全隐患。

2、弱口令和口令复用问题在内网比较突出

本月任务中目标内网弱口令和口令复用问题依旧比较突出，弱口令通常指容易被别人猜测到或被破解工具破解的口令。对攻击者而言，弱口令爆破已成为一种快速有效的攻击手段，因为利用弱口令可以毫无难度地直接获取目标网络系统的接入控制权限，最终访问到用户权限内的任何资源，并可以在此基础上进一步开展攻击渗透。

3、未授权访问漏洞是外部成功突破的重要因素

本月任务中，多个行业网络的不同外部业务系统存在未授权访问问题，未授权访问漏洞多因对外部接入的安全配置或权限认证的地址、授权页面存在漏洞导致其他用户可以直接访问从而引发重要权限可被操作、数据库或网站目录等敏感信息泄露，且传统的授权认证体系无法根据用户属性、用户行为及环境状态进行用户权限动态控制，导致授权认证机制成为被外部攻击成功突破的重要因素。

4、敏感信息泄露是严重的安全风险

本月任务中目标网络敏感信息泄露问题较为严重，以 Gitlab 开发源码为主，这些源码包含很多重要业务系统、应用平台的关键逻辑架构、函数调用实现方法和数据处理流程等关键信息，甚至包含一些极其敏感的认证信息，这些信息的泄露会给目标网络带来严重的安全威胁，极易被用来进行针对性的快速突破渗透。

5、钓鱼攻击是实现网络突破的有力辅助

本月任务中主要通过钓鱼攻击来实现对目标网络的打点突破，向前期信息搜集的目标内部人员邮箱、客服平台、微信公众号发送植入木马的文件，诱导目标人员点击钓鱼文件，使木马在对方主机上运行回连，实现对目标主机的远控，以此为支点进一步渗透目标内网。

6、内部核心业务网络纵深防御不足

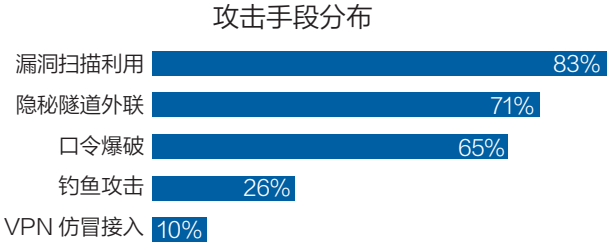
本月任务中目标的内部核心业务网络纵深防御不足，存在对关键业务网络接入缺乏安全过滤措施情况，主要表现在互联网侧业务系统被突破后可以直接扫描探测核心业务内网；被钓鱼攻击成功后可以通过非关键人员主机直接访问一些关键业务系统或网络设备。内网纵深防御不足，将极大地削弱对核心业务网络的保护。

7、攻击行为监测手段覆盖存在盲区

虽然各单位都部署了流量安全检测设备，但主要监测点分布于互联网边界及核心交换位置，普遍存在监测范围覆盖不够或加密流量无法监测的问题。一些内部网络子区域没有监测手段，通过控制子区域的一台服务器进行区域内攻击尝试时，监测能力消失，攻击成本大幅降低；部分应用系统采用了加密通信措施，攻击行为也会随之加密，流量监测设备无法监测。据此，多数单位尚未建成全覆盖、全透明的监控体系。

三、主要攻击手段分析

基于本月奇安信 Z-Team 团队实战成果分析，对目标网络的外网突破，多采用互联网侧系统漏洞利用和钓鱼攻击实现，内网横向拓展则以隐蔽隧道外连、内网漏洞利用、弱口令和口令复用等手段为主。使用的主要技术手段分布如下。



1、漏洞扫描利用

本月任务中发现，大部分被攻陷目标是因为互联网侧应用存在漏洞，且可被利用进行突破渗透。漏洞以历史漏洞为主，多因Web应用或系统组件更新不及时造成。

2、隐蔽隧道外联

本月任务中因大部分部署于内部网络的目标无法通过外网直接访问，需要借助端口、隧道技术等手段实现转发通信，对于网络功能区划分严格、核心业务隔离措施完善的内部网络，通常需要两到三层的通道转发，才能实现对目标核心业务内网的渗透。

3、口令爆破

本月任务中口令复用或弱口令是内网横向移动的有效手段，内网经常部署大量同样类型的服务器或应用安全设备，通过搜集目标网络中各种设备安装、登录的默认口令、弱口令来分析其密码组合规律，从而实现快速爆破。弱口令、口令复用问题是网络安全防护意识不足引起的。

4、钓鱼攻击

本月任务中对客服、人事、财务或商务这些网络安全知识基础薄弱的人员进行钓鱼攻击，因其对来自外网的安全威胁缺乏足够的认识，造成其十分容易被钓鱼成功，最终实现外部突破。

5、VPN 仿冒接入

本月任务中由于目标行业限制，VPN使用范围有限，只有少量目标业务网络使用 VPN 组网，攻击手段包括外网 VPN 网关漏洞利用、内网口令复用获取认证信息，实现 VPN 网络仿冒接入渗透。

四、典型攻击手段实现案例

1、漏洞扫描利用

（1）某目标 VMware vCenter 系统存在 CVE-2021-22005 漏洞，通过该漏洞利用获取服务器管理员权限，并可控虚拟机 53 台。

（2）某目标综合网管系统存在 AMF 命令执行漏洞，可通过漏洞获得服务器 root 权限及该系统 oracle 数据库权限。

（3）某目标码头生产管理系统存在 Shiro 反序列化漏洞，通过该漏洞利用获得 5 万条船舶数据及可控制船舶调度消息广播等。

2、口令爆破

（1）某目标域控服务器存在通用口令，通过漏洞利用可获取服务器管理权限，直接控制域内 425 台终端计算机及 2 台域控制器。

（2）某目标内网 MySQL 数据库服务器存在弱口令问题，通过弱口令爆破可成功控制内网 60 余台数据库服务器。

（3）某目标外网业务工作培训平台存在弱口令问题，通过弱口令爆破可登录业务后台并进一步拓展控制平台服务器。

3、钓鱼攻击

（1）对某目标邮箱、QQ 群群发钓鱼文件，并成功上线5台主机，可控制目标主机，获取目标网络突破支点。

（2）对某目标信息收集并通过添加微信好友等方式发送钓鱼木马，成功上线 4 台办公终端，登录其中一台终端可发现 12 万用户的敏感信息，包括姓名、 身份证号、银行卡号等。

（3）通过伪造某目标邮箱相似邮箱，发送关于调查疫苗接种情况话题的钓鱼邮件，成功搜集到该目标公司员工的个人信息，包括姓名、电话、身份证号、家庭住址等。

4、VPN 仿冒接入

（1）某目标外网 VPN 网关存在默认密码漏洞，利用漏洞获取 VPN 网关控制权限，进一步通过 VPN 仿冒接入目标内网。

政策篇

国内，信安标委发布十余项数据安全国家标准，围绕多个技术场景、行业场景规范数据安全保护要求；

国际上，美国政府发布 2022 年版《国家安全战略》，说明了为加强国家网络安全所采取的一系列措施，并提及了外国对手所构成的网络威胁挑战。

国内

《汽车数据处理安全要求》等 14 项网络安全国家标准获批发布

10 月 14 日，根据中华人民共和国国家标准公告（2022 年第 13 号），全国信息安全标准化技术委员会归口的 14 项国家标准正式发布。具体包括：个人信息安全工程指南，步态识别、基因识别、声纹识别等 4 项技术场景数据安全要求，汽车、即时通信、快递物流等 7 项行业场景数据安全要求，以及 2 项 ISO/IEC 27033 的等同采用标准更新版。

中国民航局印发《关于民航大数据建设发展的指导意见》

10 月 9 日，中国民用航空局印发《关于民航大数据建设发展的指导意见》（简称《指导意见》），旨在进一步加强民航大数据发展的顶层设计，指导行业更好地开展民航大数据建设工作。《指导意见》阐明了数据安全体系建设主要任务，分为强化安全管理责任、提升安全保障能力。具体包括健全网络安全、保密监测预警和密码应用安全性评估机制，建设动态监控、主动防御、协同响应的民航大数据安全技术保障体系，加强数据全生命周期安全管理和技术防护，强化重大数据安全事件应急处置机制。

国家标准《信息安全技术 软件供应链安全要求》公开征求意见

9 月 30 日，信安标委发布国家标准《信息安全技术 软件供应链安全要求》征求意见稿，向社会公开征求意见。本文件给出了软件供应链安全保护目标，规定了软件供应链组织管理和供应活动管理的安全要求，适用于指导软件供应链中的需方、供方开展组织管理和供应活动管理。该文件提出，软件供应链安全保护目标是提升软件产品或服务中断供应等风险管理能力、供应活动引入的技术安全风险管理能力、软件供应链数据安全风险管理能力。

信安标委发布《网络安全标准实践指南—健康码防伪技术指南》

9 月 28 日，为落实疫情防控政策，针对健康码伪造现象给疫情防控工作带来的严重安全挑战，信安标委秘

书处组织编制了《网络安全标准实践指南——健康码防伪技术指南》。该《实践指南》给出了现场核验场景下健康码防伪的技术指南，指导健康码服务的技术提供方提高防伪能力，提升整体安全水平。

国家标准《信息安全技术 网络安全众测服务要求》公开征求意见

9 月 27 日，信安标委发布国家标准《信息安全技术 网络安全众测服务要求》征求意见稿，向社会公开征求意见。该文件确立了网络安全众测服务的角色及其职责，描述了服务流程，规定了服务要求，适用于众测需求方、众测组织方、授权测试方和众测审计方开展网络安全众测服务时使用。该文件提出，众测服务过程面临的主要安全风险包括授权测试方行为不可控、系统正常运行受到影响、敏感信息泄露，并给出了降低风险的安全要求。

美国政府发布加强美国信号情报活动保障措施行政令

10 月 7 日，美国总统拜登签署了《关于加强美国信号情报活动保障措施的行政命令》，指示美国将采取的步骤，以落实拜登总统和欧盟委员会主席冯德莱恩于 2022 年 3 月宣布的美国在欧盟－美国数据隐私框架下的承诺。该行政令增加了对美国信号情报活动的进一步保障；颁布了通过信号情报活动所收集个人信息的处理要求；要求美国情报界成员更新其政策和程序；为根据该行政令指定的合格国家和区域经济一体化组织的个人增设多层保护机制；呼吁隐私和公民自由监督委员会审查情报界的政策和程序。

美国政府发布 2022 年版《国家安全战略》

10 月 12 日，美国白宫公布了拜登政府首份《国家安全战略》正式文件，重申了加强国家数字防御和打击网络犯罪分子的承诺。该战略详细说明了为加强国家网络安全所采取的一系列措施，并简略提及了外国对手所构成的网络威胁挑战。该报告的发布时间因俄乌冲突被推迟了几个月。国内媒体《环球时报》评论称：“与中国的竞争思维贯穿了（报告）每一章”。

尼日利亚发布《2022 年数据保护法》草案

10 月 4 日，非洲人口大国尼日利亚发布《2022 年数据保护法》草案，概述了个人数据保护的法律框架。该草案将建立尼日利亚数据保护委员会来监管个人数据处理，并概述了处理个人信息的原则，主要内容包括进行数据保护影响评估；任命数据保护官员；违规通知和跨境数据传输限制；调查和民事救济措施在内的执法能力等。

印度尼西亚通过《数据隐私法》，刑罚最高可监禁六年

9 月 20 日，在国内遭遇数起重大违规事件数月后，印度尼西亚议会审议通过了该国首个《数据隐私法》。《数据隐私法》共 16 章 76 条内容。该法规定，数据处理者因泄露或滥用个人信息可最高监禁 5 年，为谋取利益而伪造个人数据可最高监禁 6 年，发生数据泄露后可对公司处以 2% 年收入的罚款。印度尼西亚是东南亚地区第 5 个对个人数据保护单独立法的国家。 安

合规！冲刺！

—2022 网络安全合规指南

网络安全合规是实现网络安全、保障国家安全的基础，我们要以更高水平的安全为发展来托底。

政策解读

重磅解读：网络安全“合规”建设迫在眉睫的深层因素

作者 战略规划设计院

《说文解字》曰，“规，有法度也。”《孟子·离娄章句上》提到，“不以规矩，不能成方圆”，《韩非子·解老》也指出，“万物莫不有规矩”。规矩就是法度与礼仪，它无处不在，没有规矩，难成方圆；没有规矩，天下就会大乱。

现实世界如此，虚拟数字空间同样适用，在网络安全（注：本文中的网络安全是广义概念，即CyberSecurity）行业约30年的发展历程中，合规始终是一个极其重要的安全发展驱动引擎。1994年2月发布的《中华人民共和国计算机信息系统安全保护条例》，是我国第一个计算机安全法规。2007年《信息安全等级保护管理办法的发布，标志着等保1.0时代正式开启，被公认为是第一轮网络安全行业兴起的起点。

此后，网络安全法律法规伴随着行业高速成长而不断完善和丰富。从2017年6月实施的《中华人民共和国网络安全法》，再到2019年12月实施的网络安全等级保护制度2.0标准（简称等保2.0），以及2021年连续实施的《关键信息基础设施安全保护条例》《中华人民共和国数据安全法》，《中华人民共和国个人信息保护法》等。无论是政策法规、规章条例的数量之多，还是近期政策推出的频度之密，都凸显了网络安全合规的重要性和紧迫性。

2022年9月14日，实施了5年多的《网络安全法》迎来首次修改。其中包括进一步压实网络安全责任、大幅提高重大网络安全事故的罚款幅度、处罚力度与公司营业额挂钩、增加禁业处罚措施，增加对关键信息基础设施运营者违法行为罚则等，这势必将显著提升对大型政企机构对于网络安全的重视程度。

序号	日期	名称
1	1994.2.18	中华人民共和国计算机信息系统安全保护条例
2	2007.6.22	信息安全等级保护管理办法
3	2017.6.1	中华人民共和国网络安全法
4	2019.12.1	网络安全等级保护制度2.0国家标准
5	2020.1.1	中华人民共和国密码法
6	2020.6.1	网络安全审查办法
7	2021.9.1	**关键信息基础设施安全保护条例**
8	2021.9.1	网络产品安全漏洞管理规定
9	2021.9.1	**中华人民共和国数据安全法**
10	2021.11.1	**中华人民共和国个人信息保护法**

图：我国重要的网络安全政策法规

国家相关部门为何近年来显著加大网络安全的合规力度，其背后的深层逻辑又有哪些呢?

内外部形势严峻 网络安全加强合规建设迫在眉睫

哲学认为，事物的发展是内外因共同起作用的结果。网络安全在合规驱动的道路上，至少有国际外部环境、国家战略要求，数字化经济发展、威胁形式变化等多重因素的联合驱动。

首先是国际环境波云诡谲，网络对抗威胁日益严峻。

9月5日，中国相关部门对外宣布，此前西北工业大学声明遭受境外网络攻击，攻击方是美国国家安全局（NSA）特定入侵行动办公室（TAO）。此后国家计算机病毒应急处理中心与北京奇安盘古实验室对此次入侵

事件进一步深入分析，在最新的调查报告中，美国实施攻击的技术细节被公开：即在 41 种网络武器中名为“饮茶”的嗅探窃密类网络武器，就是导致大量敏感数据遭窃的最直接“罪魁祸首”之一。

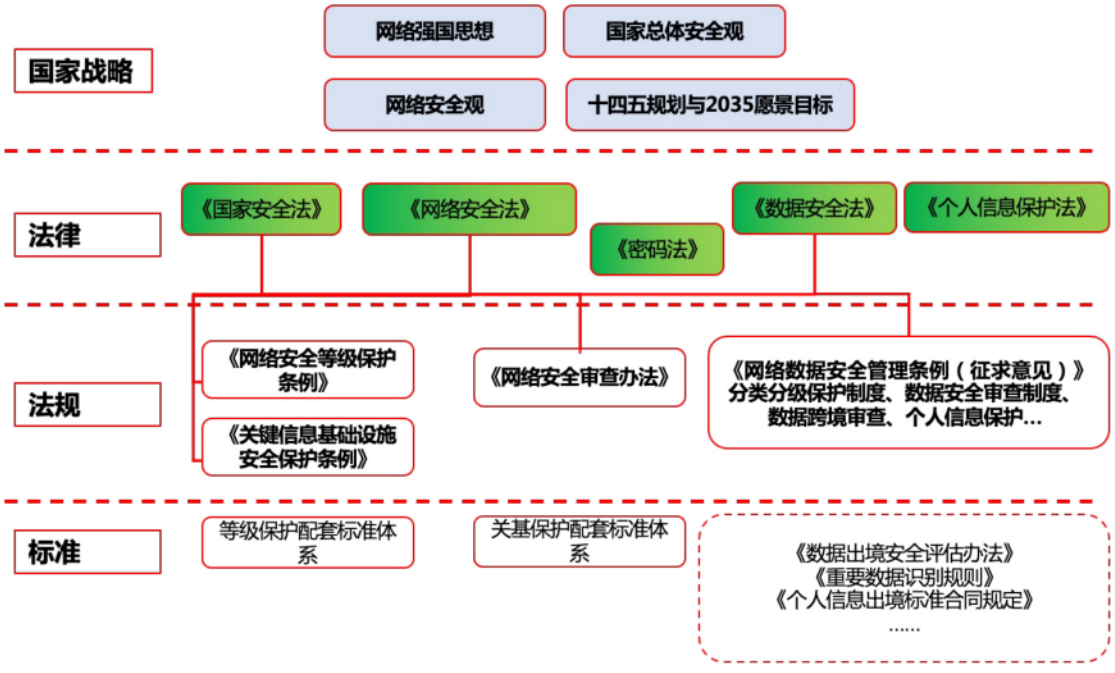
当前，世界百年未有之大变局正在加速演进，和世纪疫情交织叠加，国际环境日趋复杂，网络霸权主义对世界和平与发展构成威胁，全球产业链、供应链遭受冲击，网络空间安全面临的形势持续复杂多变。数字化空间的对抗已成为大国交锋的重要战场，网络安全已成为国家安全的重中之重。这也就不难理解我国在平衡安全与发展之间关系时的逻辑。强化安全法律体系构建与合规要求，如何强调其重要性都不为过。

其次是数字化潮流大势所趋，安全底板重要性凸显。

蓬勃发展的“数字经济”正成为拉动中国经济增长的新引擎。根据中国信通院发布的报告显示，2021 年，我国数字经济规模达到 45.5 万亿元，同比名义增长 16.2%，GDP 的占比由 2005 年的 14.2% 提升到 2021 年的 39.8%。数字经济发展速度之快、辐射范围之广、影响程度之深前所未有，正在成为重组全球要素资源、重塑全球经济结构、改变全球竞争格局的关键力量。

数字经济的高速发展离不开国家宏观规划和政策的支撑。2021 年 3 月，“中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要”获表决通过并正式发布。其中第五篇“加快数字化发展 建设数字中国”，提出迎接数字时代，激活数据要素潜能，推进网络强国建设，加快建设数字经济、数字社会、数字政府，以数字化转型整体驱动生产方式、生活方式和治理方式变革。

在本纲要中，“安全”一词共计出现 175 次，仅次于出现 468 次的“发展”、349 次的“建设”、206 次的“制度”，成为纲要中排名第四的高频热词。在 175 次提及安全相关的内容中，有 14 次与网络安全相关，5 次与数据安全相关。在“加快数字化发展 建设数字中国”的篇章中，专门对网络安全保护进行了阐述；在“统筹发展与安全 建设更高水平的平安中国”篇章，也给出了



图：国家战略与网络安全法律法规概览

“全面加强网络安全保障体系和能力建设”的阐述。可见，网络安全已成为国家、社会发展面临的重要议题，建设“安全中国”也将成为十四五规划中的战略重点和发展方向，更带来了网络安全建设的巨大机遇。

2022 年 4 月，《 中共中央国务院关于加快建设全国统一大市场的意见 》（ 以下简称《 意见 》）提到，要加快培育数据要素市场，建立健全数据安全、权利保护、跨境传输管理、交易流通、开放共享、安全认证等基础制度和标准规范，深入开展数据资源调查，推动数据资源开发利用。《 意见 》强调，要把安全贯穿数据治理全过程，守住安全底线，明确监管红线，加强重点领域执法司法，把必须管住的坚决管到位。要构建政府、企业、社会多方协同治理模式，强化分行业监管和跨行业协同监管，压实企业数据安全责任。

2022 年 6 月 22 日，中央全面深化改革委员会第二十六次会议审议通过了《 关于构建数据基础制度更好发挥数据要素作用的意见 》等，对数据确权、流通、交易、安全等方面做出部署。会议明确，数据基础制度建设事关国家发展和安全大局，要维护国家数据安全，保护个人信息和商业秘密，促进数据高效流通使用、赋能实体经济，统筹推进数据产权、流通交易、收益分配、安全治理，加快构建数据基础制度体系。

与此同时，国务院印发《 关于加强数字政府建设的指导意见 》（ 以下简称《 指导意见 》），就主动顺应经济社会数字化转型趋势，充分释放数字化发展红利，全面开创数字政府建设新局面作出部署。在构建数字政府全方位安全保障体系方面，《 指导意见 》强化安全管理责任，落实安全制度要求，提升安全保障能力，提高自主可控水平，筑牢数字政府建设安全防线。

最后，网络空间威胁形势日新月异，影响范围与维度不断扩展，也是网络安全政策法规密集出台的又一大推动因素。

近年来，安全攻击呈现出以下四个新趋势。

第一是勒索攻击事件呈现显著上升趋势。相关数据统计，2021 年平均每 11 秒就有一个企业受到勒索病毒攻击。而奇安信应急响应中心统计的数据也显示，2021 年，大中型政企机构的应急响应事件中勒索攻击占到了近 30%。

第二是数据窃密事件呈指数级攀升。2022 年 4 月，国家安全机关公布，有间谍窃取我国电信运营商、航空公司等单位的部分数据并发送至境外，严重威胁到我国关键基础设施的数据安全。IBM 发布的《 2021 年数据泄露成本报告 》指出，2021 年每起数据泄露事件带来的平均损失高达 424 万美元，同比增加 10%，达到了七年来的最大增幅。

第三是有组织的 APT 攻击威胁不减。之前国家计算机病毒应急处理中心披露的《 西北工业大学遭受美国 NSA 网络攻击调查报告 》，其幕后是“饮茶”嗅探窃密工具与 Bvp47 木马程序其他组件配合实施联合攻击，堪称典型的 APT 攻击。另一起震惊全球的 APT 事件是，9 月 7 日，北约成员国阿尔巴尼亚宣布与伊朗断绝外交关系，缘由是伊朗 APT 组织在 7 月对阿国进行了大规模网络攻击 , 这是世界上第一起因网络攻击导致两国断交的事件。

第四是供应链安全已成为网络安全的新战场。根据行业估计，供应链攻击现在占所有网络攻击的 50%，2021 年同比激增了 78%。多达三分之二的公司经历了至少一次供应链攻击事件，平均成本达 110 万美元。美国的 Solarwinds 供应链安全事件，也使得全球看到了这类攻击手段的深度应用，促使各重点行业，从这个新维度视角考虑供应链安全领域。Verizon 发布的《 2021 年数据泄露调查报告 》显示，62% 的系统入侵事件是由供应链造成的。

从合规体系完善到实际效果落地尚存在三大缺失

面对复杂而严峻的网络安全威胁形式，当前我国各个行业的合规落地实施仍存在诸多软肋和不足，具体表现在三个方面。

第一，网络安全的主体责任未压实。

对于任何一家政企机构而言，网络安全事件的发生

是一个概率事件，因此考虑到投入产出比，在很多客户看来，投资网络安全至少在明面上并不是一个“非常划算”的生意。即便是在《中华人民共和国网络安全法》正式实施以后，其最高罚款也不超过 100 万元，对于大中型企业尤其是各行业的头部公司而言，相较于复杂的网络安全技术与人才的投入，其处罚力度是远远不够的。

这就带来一个问题，网络安全主体责任并未压实。尤其越是头部的大型企业和政府机构，其发生网络安全事故后导致的后果也越严重，不仅是经济损失，更多时候所造成的国家安全与社会民生影响往往更为严重。这也是为什么在《关基保护条例》中，特别强调了从关基运营者的主体责任，以及保护工作部门的本行业、本领域监测预警与指导任务。

9 月 14 日，国家互联网信息办公室发布了关于修改《中华人民共和国网络安全法》的决定（征求意见稿），本次修改主要有以下几点。

一是完善违反网络运行安全一般规定的法律责任。并且拟调整违反网络安全保护义务或导致危害网络运行安全等后果的行为的处罚种类与处罚服务，使得罚款激增，对企业的罚款从最高 100 万提高到 5000 万或上一年度营业额的 5%，并可以责令暂停相关业务进行停业整顿，甚至吊销相关业务许可与营业执照。对直接负责的主管人员从最高 10 万元提高到 100 万元。

二是新增禁业规定，对直接负责的主管人员和其他直接责任人员，可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员或者从事网络安全管理和网络运营关键岗位的工作。

三是修改关键信息基础设施安全保护相关的法律责任制度。

四是更加注重法律的衔接，尤其与《数据安全法》《个人信息保护法》等相关新颁布法律的一致性。

可以预见的是，考虑到综合了 5000 万与营业额 5% 的顶格处罚，以及停业整顿、对于相关管理人员的从业禁止的综合处罚，即便是头部政企机构也不得不重新审视自己的网络安全责任落实与建设情况。

第二，网络安全“能力体系”的亟待完善。

需要注意的是，网络安全从法规到落地执行，需要大量的能力支撑，这些能力中包括技术、管理、运行能力，这种综合能力体系的构建，就需要有框架、参考架构、标准、指南作为指导。

近两年来我国网络安全法律法规完善速度非常快，已经走在了全球前列，但在网络安全能力体系的建设上，相比最先进的体系而言，中间这层的能力指引缺失却在一定程度上阻碍了我国网络安全整体水平的进步。

2021 年 5 月，美国总统拜登签署《改善国家网络安全的行政命令》（以下简称“行政令”），提出多项行动以加强美国网络安全防御能力，包括情报共享、零信任架构、供应链安全事件的防范等多个方面，解决美国当前易受网络攻击的安全问题。

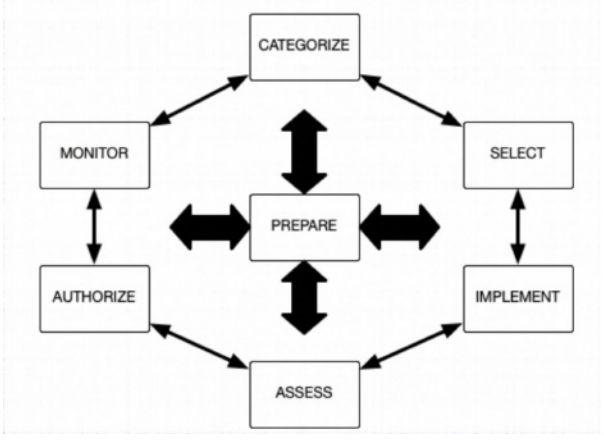
在这些方面，美国都有相对完善的参考架构与技术指南作为指引。

例如，在关基保护方面，2018 年美国国土安全部专门整合资源组建了“网络安全与基础设施安全局（CISA）”，在关基保护的政策制定、防御协同、能力指南、情报共享、安全演习等方面发挥作用。除了拜登政府《改善国家网络安全》行政令，CISA 也发布了《云计算安全技术参考架构》《零信任成熟度模型》；2021 年 2 月拜登签署《确保信息和通信技术及服务供应链安全》的行政令，NIST 也快速着手制定相关标准，2022 年 9 月《利用安全的软件开发时间增强软件供应链安全行》的备忘录随即出台；2022 年，发布了《2022 年关键基础设施网络事件报告法案》。而在这之前，美国在关基保护的范围划定、保护体系建立方面早已陆续出台了各类的政策、法案、技术指南、标准等体系化内容。覆盖面宽，落地管理细节依据较为完整，且配套的能力体系构建指引、相关标准规范丰富。

在威胁情报方面，美国联邦系统安全控制建议（NIST 800-53）、美国联邦网络威胁信息共享指南（NIST 800-150）、STIX 结构化威胁表达式、CyboX 网络可观察表达式，以及指标信息的可信自动化交换 TAXII 等都为国际间威胁情报的交流和分享提供了可靠参考。而这些标准，不仅得到了包括 IBM、思科、

戴尔、大型金融机构及美国国防部、国家安全局等主要安全行业机构的支持，还积累了大量实践经验，在实践中不断优化。更是有如美国情报共同体这样的组织机制来进行支撑。

在零信任方面，早在 2021 年 5 月，美国总统签署了行政命令，强制要求政府部门全面迈向零信任架构。与此同时，美国国家标准与技术研究院（NIST）在发布《零信任安全架构标准》之后，再次为联邦管理人员发布了一份规划指南，概述了如何将 NIST 风险管理框架（RMF）应用于实施零信任架构。RMF 提出了一种方法，其中包括一组集成到企业风险分析、规划、开发和运营中的步骤和任务。这些步骤分为七个行动：准备、分类、选择、实施、评估、授权和监控。



图：美国 NIST 风险管理框架七个步骤

在供应链安全方面，2022 年 5 月 5 日 NIST 发布了新版《系统和组织网络安全供应链风险管理实践》，旨在提供识别、评估和应对整个供应链各级组织网络安全风险的指导，提高组织在供应链内部和整个供应链中管理网络安全风险的能力。它是 NIST 对有关网络安全的行政命令回应的一部分。修订后的标准主要面向产品、软件和服务的购买者及最终用户。该指南有助于各组织将网络安全供应链风险考虑和要求纳入其收购流程，并强调了风险监控的重要性。

第三，常态化、实战化的深度运营缺失。

网络安全最终的效果需要从实战化的安全运营中体现，从 2016 年开始，我国有关部门都会在全国范围内组织一次较大规模的实战攻防演习，用以检验部分重要机构的网络安全建设成果和实战化攻防水平。除此之外，各省市、行业等自行组织的小范围实战攻防演习，更是数不胜数。

能够看到的是，历经数年的发展，实战攻防演习的水平越来越高，战况也越来越激烈，各种攻防手段层出不穷，对推动我国整体实战化水平和产业发展，起到了巨大的推动作用。

正如部分业内专家所谈论的那样，伴随着时代大潮，还有很多问题也隐藏其中。比如，面对演习期间高频度的攻击，作为防守方不得不严阵以待、如履薄冰，加派人手修补潜在的安全隐患，处置每一个可疑的告警。而随着演习的结束，所有运营手段都又恢复成“老样子”：对那些高危甚至已经发生在野利用的漏洞视而不见、需要进行加固的策略无持续优化、安全设备的检测规则也不及时更新……

演习的主要目的是为了帮助防守方检查哪里还存在着不足，因此在演习结束后，大量机构都会根据自身情况采购最需要的产品和服务。但网络安全的本质是人与人的对抗，缺乏常态化和实战化运营的设备堆砌，很难起到保障企业网络安全的作用。如此一来，原本查漏补缺的目的并未达到，借演习来提升常态化、实战化安全能力的目标也随之落空。

推动合规落地 需做好三项工作

面对日益严峻的外部形势和错综复杂的安全威胁，奇安信认为，广大政企机构应积极推动以下三项措施，尽快补齐合规短板，构筑牢固的安全防线。

第一步，夯实地基，合规与业务并重。

一直以来，很多企业都对合规存在误解，认为合规是网络安全工作的目标。事实上，合规仅仅是网络安全的基本要求和底线。企业不遵守安全规范，就像没有打

牢地基，注定无法长久。

企业需要深刻认知到，安全的本质是要解决业务连续性和安全风险相关的问题，脱离业务就很难让安全达到很好的效果。企业在落实网络安全合规建设的同时，还需要从业务视角出发，基于动态风控的思路，实现面向业务风险的安全治理，最终达到守牢安全底线和保障业务经营的双重目标。

第二步，角色转化，健全组织机制。

从 9 月份的《网安法修订稿》中可以看出，有两个信息和企业的经营负责人紧密相关。第一是顶格处罚激增，对企业罚款从最高 100 万元提高到 5000 万或上年度营业额的 5%，甚至直接造成企业运营停摆。第二，《网安法修订稿》特别增加了“禁止其在一定期限内担任相关企业的董事、监事、高级管理人员或者从事网络安全管理和网络运营关键岗位的工作”，有力强化对涉及违法行为的相关管理人员的惩戒效果。可见，网络安全是否合规，安全责任是否压实，不仅直接关乎企业的经营指标、利润盈亏，同时还和企业管理者的个人职业生涯密切相关。

为了避免企业遭受可能高达数十亿级的巨额罚款，以及管理者遭受禁业处罚，政企一把手需要对三个问题了如指掌，即组织是否健全，责任是否落实，技术能力支撑是否到位。

具体落实上，企业应组建“网络安全合规专项工作组”，合规的第一责任人，需要从单纯的 IT 部门、网络安全部门负责人，上升到政企机构的一把手、经营管理负责人。通过一把手领导牵头，建立一个横跨公司管理、法务、技术、业务等多个部门的综合组织，才能将网络安全合规工作责任落到实处，满足监管需求，并避免安全和业务相脱节。

第三步，补齐短板，兼顾长远，体系规划。

据统计，国内 85% 以上的政企机构在面对最新的数据安全法律法规的合规要求时，最需要“先理后治、补短固底”。“补短板、防违规”，是网络安全与数据安全的当务之急，更是合规建设的突破口。滴滴、知网等频遭审查或处罚的事件说明，企业迫切需要尽快自查隐藏的合规风险，分析问题原因，及时补齐安全短板，才能最大程度降低监管部门处罚的风险。

在补齐短板的同时，企业还需兼顾长期的体系化建设，以及常态化的安全运营。过去，企业只要按照要求部署产品，就是做到了合规，这就导致很多企业仅仅把合规当成“应试”和“交差”，觉得只要通过检查和测试就万事大吉，没有把后续的实际效果和可持续性考虑在内，使得合规流于形式，面对新的监管和网络攻击时依然千疮百孔。

完整的网络安全能力体系的构建，与“新管理”的落地，和实战攻防演习不同，它是一个长期、有序、常态化的过程。在数字化时代，缺乏能力体系支撑、安全技术控制点的合规条文，是难以最终落地的。所以网络安全的新管理，也需要从传统的“条文式管理”发展到有能力体系支撑的、有数据结果驱动的“效果型”管理上来。

在这个过程中，除了企业和监管单位的努力，还需要充分借助外部的专业力量，依托专业网络安全公司，以及第三方法律机构的参与和支持，对合规制度流程不断完善，对人员技术能力不断提升，对各类安全风险持续跟踪及修复，才能从长远角度提升企业的安全水平。

结束语：

从无法可依到有法可依，从合规性驱动到合规性和强制性驱动并重，以《网络安全法》《数据安全法》《个人信息保护法》等为代表的网络空间安全法治建设，为维护国家总体安全、抵御网络空间各种不确定性因素和未知风险发挥了重要作用。然而，在当前国际严峻的威胁形势下，网络安全面对的挑战依然严峻，合规建设任重而道远。只有落实体系化建设，实现国家指导、行业保护、网络服务机构支持、运营者落实等多方协同，才能落实相关合规监管要求，筑牢网络安全底板，化解重大风险，保障业务正常运转，为我国数字强国之路保驾护航。

政策解读

顶格罚款 5000 万！《网络安全法》修改体现五大变化

作者 解决方案中心

2022 年 9 月，中央网信办会同相关部门起草《关于修改〈中华人民共和国网络安全法〉的决定（征求意见稿）》（以下简称《征求意见稿》）。《网络安全法》是我国首部关于网络安全工作的基本大法，自 2017 年 6 月 1 日正式施行以来，为我国网络空间安全治理提供了有力的法律保障。本次修订是为了与 2021 年相继修订制定实施的《行政处罚法》《数据安全法》《个人信息保护法》等法律衔接协调。

本次修订主要针对《网络安全法》中“第六章 法律责任”部分条款进行了修订完善，是我国加强网络安全工作的又一有力举措，将进一步完善我国网络安全法律法规体系。

本次修改主要有以下几点。

第一，顶格罚款金额激增，对企业罚款从最高 100 万提高到 5000 万或上一年度营业额的 5%，对直接负责的主管人员从最高 10 万元提高到 100 万元，直接与《个人信息保护法》接轨。

第二，新增禁业规定，对直接负责的主管人员和其他直接责任人员可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员或者从事网络安全管理和网络运营关键岗位的工作。

第三，新增通报批评，违法者除了被有关主管部门责令改正、给予警告，还新增了通报批评的行政处罚形式。

具体而言，征求意见稿主要体现以下五大变化。

一、增加与营业额挂钩的处罚措施，显著提升对大型企业组织的震慑力度。

现有《网络安全法》针对违法主体的处罚额度一般不超过 100 万，对于大型企业组织来说难以达到与之规模相匹配的惩戒力度。《网安法修订稿》针对违反网络运行安全一般规定的网络运营者、关键信息基础设施的运营者及违反网络信息安全义务的网络运营者，均增加了在特定违法情况下“处上一年度营业额百分之五以下罚款”的表述，与去年出台的《个人信息保护法》相关处罚措施相一致，这将对大型企业组织遵守《网络安全法》相关规定产生极大的震慑作用，有力提升法律的权威性和威慑力。

二、增加禁业处罚措施，有力强化对涉及违法行为的相关管理人员的惩戒效果。

对于情节特别严重的违反网络运行安全一般规定的网络运营者和违反网络信息安全义务的网络运营者，除了保留对相关管理人员的罚款措施，《网安法修订稿》特别增加了“禁止其在一定期限内担任相关企业的董事、监事、高级管理人员或者从事网络安全管理和网络运营关键岗位的工作”，有力强化对涉及违法行为的相关管理人员的惩戒效果。

三、整合提升同一大类违法行为的行政处罚幅度，就高不就低。

例如，将原来第五十九条、第六十条、第六十一条、第六十二条针对违反不同条款的行为的处罚种类和幅度合并为同一表述，将几类违法主体拒不改正或者情节严重的“处一万元以上十万元以下罚款”“处五万元以上五十万元以下罚款”“处十万元以上一百万元以下罚款”不同处罚额度，统一合并提升到“处一百万元以下罚款”。

四、与其他法律法规处罚措施保持一致。

将原有关个人信息保护的法律责任修改为转致性规定：“网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十四条规定，侵害个人信息依法得到保护的权利的，依照有关法律、行政法规的规定处罚”，相关处罚主要参照《个人信息保护法》规定执行。将关键信息基础设施的运营者违反本法第三十七条规定（在境外存储网络数据，或者向境外提供网络数据的）的法律责任也修改为转致性规定，相关处罚主要参照《数据安全法》和《关键信息基础设施安全保护条例》规定执行。

五、增加兜底性条款，适应网络空间快速变化新形势。

针对《网络安全法》第七十条中“发布或者传输本法第十二条第二款和其他法律、行政法规禁止发布或者传输的信息的”情况，对法律、行政法规没有规定的情形增加了兜底性罚则，在网络环境快速变化、信息安全违法犯罪形式层出不穷的背景下，兜底条款能够保证在出现一些新型违法行为都能对应罚则。

总体而言，本次修订工作明显强化了网络安全违法行为的处罚力度，对于提升全社会（特别是大型企业组织）加强网络安全守法意识，具有极大的推动作用。

《网络安全法》原条文	拟修改内容
第五十九条 网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。	违反本法第二十一条、第二十二条第一款和第二款、第二十三条、第二十四条第一款、第二十五条、第二十六条、第二十八条、第三十三条、第三十四条、第三十六条、第三十八条规定的网络运行安全保护义务或者导致危害网络运行安全等后果的，由有关主管部门责令改正，给予警告、通报批评；拒不改正或者情节严重的，处一百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。
第六十条 违反本法第二十二条第一款、第二款和第四十八条第一款规定，有下列行为之一的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款：（一）设置恶意程序的；（二）对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的；（三）擅自终止为其产品、服务提供安全维护的。	有前款规定的违法行为，情节特别严重的，由省级以上有关主管部门责令改正，处一百万元以上五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令停止相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员或者从事网络安全管理和网络运营关键岗位的工作。
第六十一条 网络运营者违反本法第二十四条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，并可以由有关	

主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。 **第六十二条** 违反本法第二十六条规定，开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息的，由有关主管部门责令改正，给予警告；拒不改正或者情节严重的，处一万元以上十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五千元以上五万元以下罚款。	
第六十三条 违反本法第二十七条规定，从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助，尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。违反本法第二十七条规定，受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。 **第六十七条** 违反本法第四十六条规定，设立用于实施违法犯罪活动的网站、通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息，尚不构成犯罪的，由公安机关处五日以下拘留，可以并处一万元以上十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处五万元以上五十万元以下罚款。关闭用于实施违法犯罪活动的网站、通讯群组。单位有前款行为的，由公安机关处十万元以上五十万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。	违反本法第二十七条、第四十六条规定，从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助，或者设立用于实施违法犯罪活动的网站、通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息，尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。 违反本法第二十七条规定，受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

第六十四条 网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。	网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十四条规定，侵害个人信息依法得到保护的权利的，依照有关法律、行政法规的规定处罚。
第六十五条 关键信息基础设施的运营者违反本法第三十五条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。	关键信息基础设施的运营者违反本法第三十五条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下或者上一年度营业额百分之五以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。
第六十六条 关键信息基础设施的运营者违反本法第三十七条规定，在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。	关键信息基础设施的运营者违反本法第三十七条规定，在境外存储网络数据，或者向境外提供网络数据的，依照有关法律、行政法规的规定处罚。
第六十八条 网络运营者违反本法第四十七条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处十万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第四十八条第二款规定的安全管理义务的，依照前款规定处罚。	违反本法第四十七条、第四十八条、第四十九条规定的网络信息安全保护义务，或者不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息采取停止传输、消除等处置措施的，或者不按照有关部门的要求对网络存在较大安全风险和发生安全事件采取措施的，由有关主管部门责令改正，给予警告、通报批评，没收违法所得；拒不改正或者情节严重的，处一百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十九条 网络运营者违反本法规定，有下列行为之一的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款：（一）不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息，采取停止传输、消除等处置措施的；（二）拒绝、阻碍有关部门依法实施的监督检查的；（三）拒不向公安机关、国家安全机关提供技术支持和协助的。	情节特别严重的，由省级以上有关主管部门责令改正，没收违法所得，处一百万元以上五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员或者从事网络安全管理和网络运营关键岗位的工作。
第七十条 发布或者传输本法第十二条第二款和其他法律、行政法规禁止发布或者传输的信息的，依照有关法律、行政法规的规定处罚。	发布或者传输本法第十二条第二款和其他法律、行政法规禁止发布或者传输的信息的，依照有关法律、行政法规的规定处罚。 法律、行政法规没有规定的，由有关主管部门责令改正，给予警告、通报批评，没收违法所得；拒不改正或者情节严重的，处一百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。 情节特别严重的，由省级以上有关主管部门责令改正，没收违法所得，处一百万元以上五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员或者从事网络安全管理和网络运营关键岗位的工作。

政策解读

数据安全合规义务与合规建议

作者 战略推进中心

本文选取具有代表性的 6 部数据安全法律法规，从 8 个维度梳理其中的内在逻辑关系，对数据安全政策的新特点、新趋势进行深度分析，在此基础上提出推动数据安全保护的相关建议。

一、概述

《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》是上位法，涉及范围广、原则要求多，提供了基础法律依据，需要在执行过程、具体领域中进行细化；《网络数据安全管理条例（征求意见稿）》进一步细化落实数据安全管理，对多项原则要求进行细化，满足了当前日益迫切的数据安全管理需求；《汽车数据安全管理若干规定（试行）》《关于加强车联网网络安全和数据安全工作的通知》加强汽车数据、特别是车联网网络安全和数据安全管理，是汽车领域数据安全的主要制度，是上位法在具体领域的细化；《数据出境安全评估办法（征求意见稿）》进一步细化落实数据出境相关管理要求，是对当前数据出境过程中相关要求的整合细化。在两部法律颁布的当年，就配套推出了相关条例、办法、规定、通知，既体现了国家对数据安全的高度重视，也反映出加强汽车数据安全、数据出境安全的急迫性和重要性。

上述数据安全政策之间主要呈现以下三个方面关系。

执行方面。数据安全法和个人信息保护法是上位法，网络数据安全管理条例是为了执行上位法而设立的制度，给出了具体的实施路径。规定、通知、办法是在重点行业、重点领域的落实落细。对于上位法中已经明确的内容，条例、规定、通知、办法往往不再重复规定。

《中华人民共和国数据安全法》	2021 年 6 月 10 日，第十三届全国人民代表大会常务委员会第二十九次会议通过 9 月 1 日起施行
《中华人民共和国个人信息保护法》	2021 年 8 月 20 日，第十三届全国人民代表大会常务委员会第三十次会议通过 2021 年 11 月 1 日起施行
《汽车数据安全管理若干规定（试行）》	2021 年 8 月 16 日，国家网信办牵头出台
《关于加强车联网网络安全和数据安全工作的通知》	2021 年 9 月 15 日，工信部出台
《数据出境安全评估办法（征求意见稿）》	2021 年 10 月 29 日，国家网信办发布
《网络数据安全管理条例（征求意见稿）》	2021 年 11 月 14 日，国家网信办配套推出

细化方面。对于上位法中的原则要求，或者理解实施过程中需要进一步明确的内容，条例、规定、通知、办法作了进一步细化。例如，上位法中提出的“网信部门规定的条件”“网信部门规定的数量”等概念的内涵，条例都作了明确。

新增方面。条例、规定、通知、办法可以创设制度，设定行政许可，增加新的要求。例如，重要数据处理者备案要求和年度报告要求、数据出境安全管理义务、网络平台责任等。

二、主要数据安全政策的新特点新趋势

我国数据安全保护工作迈入了新阶段。数据安全政

表 0 我国主要数据安全政策与要求的分布

	概念内涵	分类分级保护	数据安全应急处置	网络安全审查	数据安全评估	数据安全管理责任	数据安全培训	数据安全审计
数据安全法	基准	基准	基准	基准	基准	基准	基准	
个人信息保护法	基准	基准	——	——	基准	基准	基准	基准
网络数据安全管理条例（征求意见稿）	新增了重要数据、核心数据、公共数据、公共信息的定义 第七十三条	细化了数据的分类分级，包括一般数据、重要数据、核心数据 第五条	细化了数据安全事件的等级，以及相应的措施 第十一条	新增了需要开展网络安全审查的情况 第十三条	细化了处理重要数据或者赴境外上市的数据处理者开展数据安全评估的频次、评估内容，增加了共享、交易、委托处理重要数据的情况 第三十二条	细化了数据安全管理机构的职责，数据安全负责人的任职条件和权力 第二十八条	细化培训主体和培训范围、频次的要求，新增了制定数据安全培训计划的要求 第四条、三十条	新增大型互联网平台运营者和国家建立数据安全审计制度的要求 第五十三条、五十八条
汽车数据安全管理若干规定（试行）	细化汽车领域个人信息、敏感个人信息、重要数据的定义 第三条	——	——	——	——	——	——	——
关于车联网网络安全和数据安全工作的通知	——	新增了建立数据管理台账的要求 第五条（第 13 款）	新增了开展应急演练和处置网络安全风险的内容 第三条（第 8 款）	——	新增了商用密码应用安全性评估、在线升级服务（OTA）安全和漏洞检测评估内容 第十条、十一条	——	——	——
数据出境安全评估办法（征求意见稿）	——	——	细化	——	细化了需要开展数据安全评估的情形 第四条	——	——	——

策呈现出一系列新特点新趋势，需要正确认识和把握方向、抓好重点，加快提升数据安全保护能力。

（一）主体概念体系更加完善，衔接统一成为重要方向

《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《网络数据安全管理条例（征求意见稿）》《汽车数据安全管理若干规定（试行）》等 4 个制度主要涉及 27 个概念内涵。《关于加强车联网网络安全和数据安全工作的通知》《数据出境安全评估办法（征求意见稿）》沿用上述法律法规的概念内涵，并未作出新的概念界定。上述法律法规中，将数据、数据处理和数据处理者的概念进行了相互衔接与细化完善。

关于数据的定义：兼顾了通用性与针对性。《数据安全法》作了通用表述；《个人信息保护法》限定到与已识别或者可识别的自然人有关的各种信息；《网络数据安全管理条例》限定到电子方式记录的信息，并拓展界定了重要数据、核心数据、公共数据、公共信息的内涵；《汽车数据安全管理若干规定（试行）》限定到汽车设计、生产、销售、使用、运维等过程中涉及的个人信息数据和重要数据，并拓展界定了个人信息、敏感个人信息、重要数据的内涵，为汽车行业提供了针对性的制度保障。

关于数据处理的定义：体现了不断发展与逐步细化。《数据安全法》《汽车数据安全管理若干规定》发布时间较早，提到了收集、存储、使用、加工、传输、提供、公开等 7 个环节；《个人信息保护法》增加了删除环节，《网络数据安全管理条例》进行了沿用。

关于数据处理者的定义：包括了界定和细化。《数据安全法》只作了分类，并未具体定义；《个人信息保护法》和《网络数据安全管理条例》，均作了描述界定，数据处理活动中自主决定处理目的和处理方式的个人和组织；《汽车数据安全管理若干规定》则具体指出了数据处理者的范围，包括汽车制造商、零部件和软件供应商、经销商、维修机构及出行服务企业等。

此外，《数据安全法》还提出了数据安全定义，指通过采取必要措施，确保数据处于有效保护和合法利用状态，以及具备保障持续安全状态的能力。《个人信息保护法》提出了自动化决策、去标识化、匿名化的定义，《网络数据安全管理条例》提出了委托处理、单独同意、互联网平台运营者、大型互联网平台运营者、数据跨境安全网关等 5 个定义，组成了相对完善的概念体系。

关于主体的明确：梳理 6 部法律法规，共涉及 26 个主体，基本实现了相关主体的全覆盖，但这些主体之间存在一定交叉，需要在后续法律法规制定过程中做好衔接统一，保证法律法规之间的执行一致性。主体清单：国家、国家机关、国家网信部门、履行个人信息保护职责的部门、设区的市级网信部门、关键信息基础设施运营者、各地区各部门、各相关企业、主管部门、监管部门、省（区、市）通信管理局、工业和信息化主管部门、个人信息处理者、个人信息处理者、数据处理者、重要数据处理者、汽车数据处理者、互联网平台运营者、大型互联网平台运营者、智能网联汽车生产企业、车联网服务平台运营企业、数据安全服务机构、检测机构、商用密码检测机构、安全评估的机构和人员、专业机构、数据安全审计专业机构。

表 1 概念分布

	数据	数据处理	数据处理者	其他
数据安全法	数据 第三条	数据处理 第三条	——	数据安全 第三条
个人信息保护法	个人信息 第四条	个人信息的处理 第四条	个人信息处理者 第七十三条	自动化决策、去标识化、匿名化 第七十三条
网络数据安全管理条例（征求意见稿）	网络数据（简称数据）、重要数据、核心数据、公共数据、公共信息 第七十三条	数据处理活动 第七十三条	数据处理者 第七十三条	委托处理、单独同意、互联网平台运营者、大型互联网平台运营者、数据跨境安全网关 第七十三条
汽车数据安全管理若干规定（试行）	汽车数据、个人信息、敏感个人信息、重要数据 第三条	汽车数据处理 第三条	汽车数据处理者 第三条	——

（二）分类分级要求更加清晰，行业试点亟需细化落实

当前，法律法规中关于数据分类分级的要求正在逐步深入。《数据安全法》中明确了国家分类分级的总体原则，即“根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护”；《网络数据安全管理条例》对各地区各部门、各相关企业都提出了进行数据分类分级的要求。但对于重要程度、危害程度的度量，分级对象的颗粒度尚无具体标准，这在一定程度上影响了具体行业领域数据安全分类分级工作的规范化开展。客观上来看，各行业的数据特点、数据量存在较大差异，推行分类分级的紧迫性与要求也不同，需要选取典型行业开展试点，在探索中不断优化完善分类分级标准。

在数据分类分级要求方面，明确了国家、各地区各部门、各相关企业的主要职责。

国家层面重点明确了数据分类分级的三项原则要求，即建立数据分类分级保护制度，将数据分为一般数据、重要数据、核心数据，对个人信息和重要数据进行重点保护，对核心数据实行严格保护。

各地区各部门重点负责本地区、本部门及相关行业、领域数据的分类分级管理。

各相关企业主要包括个人信息处理者和汽车行业相

表 2 分类分级保护的主体及职责

主体	责任范围	法律条款
国家	建立数据分类分级保护制度，…，对数据实行分类分级保护	数据安全法 第二十一条
	将数据分为一般数据、重要数据、核心数据，不同级别的数据采取不同的保护措施	网络数据安全管理条例 第五条
	国家对个人信息和重要数据进行重点保护，对核心数据实行严格保护	
各地区各部门	按照国家数据分类分级要求，对本地区、本部门以及相关行业、领域的数据进行分类分级管理	
各相关企业	严格落实网络安全分级防护要求，加强网络设施和网络系统资产管理，合理划分网络安全域，加强访问控制管理，做好网络边界安全防护	关于加强车联网网络安全和数据安全工作的通知 三（五）
个人信息处理者	对个人信息实行分类管理	个人信息保护法 第五十一条
智能网联汽车生产企业、车联网服务平台运营企业	建立数据管理台账，实施数据分类分级管理，加强个人信息与重要数据保护	关于加强车联网网络安全和数据安全工作的通知 五（十三）

关企业。个人信息处理者要对个人信息实行分类管理。汽车行业相关企业要严格落实网络安全分级防护要求，加强网络设施和网络系统资产管理，合理划分网络安全域，加强访问控制管理，做好网络边界安全防护；特别是智能网联汽车生产企业和车联网服务平台运营企业，还要建立数据管理台账，实施数据分类分级管理，加强个人信息与重要数据保护。

（三）安全应急处置分类更加精细，能力建设迫在眉睫

法律法规中对国家、主管部门、数据处理者都提出了建立应急处置机制的要求，并按照数据安全事件、数据泄露风险和网络安全事件等三类事件及其严重程度，精细化地规定了相应的应急处置要求。对智能网联汽车生产企业和车联网服务平台运营企业，还要求定期开展应急演练，及时处置安全威胁、网络攻击、网络侵入等网络安全风险。对各相关企业要求强化数据安全监测预警和应急处置能力建设，提升异常流动分析、违规跨境传输监测、安全事件追踪溯源等水平，不断提高数据安全应急处置能力。

在数据安全应急处置方面，明确了对国家、主管部门、数据处理者的具体要求。

国家层面重点明确了建立数据安全应急处置机制的要求。

主管部门应当依法启动应急预案，采取相应的应急处置措施，防止危害扩大，消除安全隐患，并及时向社会发布与公众有关的警示信息。

数据处理者要建立数据安全应急处置机制；特别是智能网联汽车生产企业和车联网服务平台运营企业，还要制定网络安全事件应急预案，定期开展应急演练，及时处置安全威胁、网络攻击、网络侵入等网络安全风险。

表 3 数据安全应急处置的主体及其职责

主体	责任范围	法律条款
国家	建立数据安全应急处置机制	数据安全法 第二十三条
主管部门	应当依法启动应急预案，采取相应的应急处置措施，防止危害扩大，消除安全隐患，并及时向社会发布与公众有关的警示信息	
数据处理者	建立数据安全应急处置机制	网络数据安全管理条例 第十一条
智能网联汽车生产企业、车联网服务平台运营企业	建立网络安全应急响应机制，制定网络安全事件应急预案，定期开展应急演练，及时处置安全威胁、网络攻击、网络侵入等网络安全风险	关于加强车联网网络安全和数据安全工作的通知 三（八）

当数据安全事件、数据泄露风险和网络安全事件发生时，将触发数据安全应急处置流程。

在数据安全事件发生时，数据处理者要及时启动应急响应机制，采取措施以防止危害扩大，消除安全隐患。并根据数据安全事件态势决定进一步的措施：若对个人、组织造成危害，要将安全事件和风险情况、危害后果、已经采取的补救措施等，以电话、短信、即时通信工具、电子邮件等方式通知利害关系人，无法通知的可采取公告方式告知；若涉嫌犯罪，要按规定向公安机关报案；若出现重要数据或者十万人以上个人信息泄露、损毁、丢失时，要在事件发生的 8 小时内向设区的市级网信部门和有关主管部门报告事件基本信息，在事件处置完毕后五个工作日内向设区的市级网信部门和有关主管部门报送调查评估报告。

在数据泄露风险发现时，数据处理者要妥善开展应急处置，并保障个人维护个人信息权益的通畅渠道。

在网络安全事件发生时，智能网联汽车生产企业和车联网服务平台运营企业要启动应急预案，采取相应的补救措施，并按照《公共互联网网络安全突发事件应急预案》等规定向有关主管部门报告。

（四）网络安全审查要求更加明确，审查内容尚需持续优化

从法律、办法再到条例，法律法规中关于网络安全审查的申报条件逐步清晰、细化，但对于需要审查的内容并未做出明确要求，需要在实践探索中持续优化。《数据安全法》第二十四条重点明确了在国家层面“建立数据安全审查制度，对影响或者可能影响国家安全的数据处理活动进行国家安全审查”的总体要求。《网络安全审查办法》提出了三种需要申报网络安全审查的情况，以及需要考虑的国家安全风险因素。《网络数据安全管理条例（征求意见稿）》提出了 4 种需要申报网络安全审查或报告的情况。

《网络安全审查办法》明确了网络安全审查重点评估采购活动、数据处理活动，以及国外上市可能带来的国家安全风险的情况。

关键信息基础设施运营者采购网络产品和服务的，应当预判该产品和服务投入使用后可能带来的国家安全风险。影响或者可能影响国家安全的，应当向网络安全审查办公室申报网络安全审查。

掌握超过 100 万用户个人信息的网络平台运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。

网络安全审查工作机制成员单位认为影响或者可能影响国家安全的网络产品和服务及数据处理活动，由网络安全审查办公室按程序报中央网络安全和信息化委员会批准后，依照本办法的规定进行审查。为了防范风险，当事人应当在审查期间按照网络安全审查要求，采取预防和消减风险的措施。

《网络数据安全管理条例（征求意见稿）》第十三条明确了申报网络安全审查的触发条件和向国家网信部门与主管部门报告的条件。

在出现公司合并、重组、分立或赴国外上市、赴香港上市，或者境外设立总部、运营中心、研发中心的情况时，须进行网络安全审查，数据处理者、互联网平台运营者要做好相应的审查申请或报告。

在公司合并、重组、分立，且汇聚掌握大量关系国家安全、经济发展、公共利益的数据资源，影响或者可能影响国家安全时，互联网平台运营者要申报网络安全审查。

赴国外上市时，只要处理个人信息达到 100 万人以上的数据处理者，均需申报网络安全审查。

赴香港上市时，影响或者可能影响国家安全的数据处理者，均需申报网络安全审查。

在境外设立总部、运营中心、研发中心的大型互联网平台运营者，要向国家网信部门和主管部门报告。该要求目前仅针对大型互联网平台运营者，即用户超过五千万、处理大量个人信息和重要数据、具有强大社会动员能力和市场支配地位的互联网平台运营者。

（五）数据安全评估要求更加落地，以评促建成为重要抓手

当前法律法规中关于数据安全评估的篇幅最大、要求最细，体现了数据安全评估的重要性，也反映出数据安全评估工作相对成熟。数据处理者、个人信息处理者是数据安全管理和个人信息保护主体，应当规范开展数据处理活动，认真落实数据安全和个人信息保护的责任义务。开展数据安全评估，以评促建，是落实数据安全主体责任的重要抓手，也是顺应国家数据安全体系建设的必然要求，是数据处理者需要抓好的重要工作。

表 4 网络安全审查触发条件及处理流程

触发条件	主体	责任范围	法律条款
采购网络产品和服务的，该产品和服务投入使用后可能带来国家安全风险的	关键信息基础设施运营者	应当向网络安全审查办公室申报网络安全审查	网络安全审查办法 第五条
赴国外上市，且掌握超过 100 万用户个人信息	网络平台运营者	必须向网络安全审查办公室申报网络安全审查	网络安全审查办法 第七条
网络安全审查工作机制成员单位认为影响或者可能影响国家安全的网络产品和服务以及数据处理活动，报中央网络安全和信息化委员会批准后，依照本办法的规定进行审查	关键信息基础设施运营者 网络平台运营者	在审查期间按照网络安全审查要求采取预防和消减风险的措施	网络安全审查办法 第十六条
汇聚掌握大量关系国家安全、经济发展、公共利益的数据资源，在实施合并、重组、分立，且影响或者可能影响国家安全时	互联网平台运营者	申报网络安全审查	网络数据安全管理条例 第十三条
赴国外上市，且处理个人信息达到一百万人以上时	数据处理者	申报网络安全审查	
赴香港上市，且影响或者可能影响国家安全时	数据处理者	申报网络安全审查	
在境外设立总部或者运营中心、研发中心	大型互联网平台运营者	向国家网信部门和主管部门报告	

在数据安全评估方面，分别对国家网信部门，省（区、市）通信管理局、工业和信息化主管部门，各相关企业、数据处理者，检测评估机构的权责义务进行了说明。

国家网信部门会同国务院有关部门根据处理数据情况对运营者进行数据安全评估，以抽查方式核验向境外提供个人信息或重要数据的类型、范围等（运营者应当以明文、可读方式予以展示）。

省（区、市）通信管理局、工业和信息化主管部门对企业履行数据安全保护义务进行监督检查。

重要数据处理者对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告。

汽车行业相关企业要自行或者委托检测机构定期开展网络安全符合性评测和风险评估，及时消除风险隐患。特别是智能网联汽车生产企业和车联网服务平台运营企

业，要开展数据安全风险评估，并向所在省（区、市）通信管理局、工业和信息化主管部门报备；智能网联汽车生产企业还要加强在线升级服务（OTA）安全和漏洞检测评估，车联网服务平台运营企业在平台被认定为关键信息基础设施后要自行或者委托商用密码检测机构开展商用密码应用安全性评估。

表 5 数据安全评估主体及职责

主体	责任范围	时间要求	法律条款
国家网信部门	会同国务院有关部门组织安全评估（因业务需要确需向境外提供重要数据时）	——	汽车数据安全管理若干规定 第十一条
	会同国务院有关部门以抽查等方式核验前款规定事项，汽车数据处理者应当予以配合，并以可读等便利方式予以展示（汽车数据处理者向境外提供重要数据，不得超出出境安全评估时明确的目的、范围、方式和数据种类、规模等）	——	汽车数据安全管理若干规定 第十二条
省（区、市）通信管理局，工业和信息化主管部门	对企业履行数据安全保护义务进行监督检查	——	关于加强车联网网络安全和数据安全工作的通知 第十三条
重要数据处理者	对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告	定期	数据安全法 第三十条
各相关企业	自行或者委托检测机构定期开展网络安全符合性评测和风险评估，及时消除风险隐患	定期	关于加强车联网网络安全和数据安全工作的通知 第五条
智能网联汽车生产企业	加强在线升级服务（OTA）安全和漏洞检测评估	——	关于加强车联网网络安全和数据安全工作的通知 第十一条
	开展数据安全风险评估，并向所在省（区、市）通信管理局、工业和信息化主管部门报备	定期	关于加强车联网网络安全和数据安全工作的通知 第十三条
车联网服务平台运营企业	认定为关键信息基础设施的，自行或者委托商用密码检测机构开展商用密码应用安全性评估		关于加强车联网网络安全和数据安全工作的通知 第十条
	开展数据安全风险评估，并向所在省（区、市）通信管理局、工业和信息化主管部门报备	定期	关于加强车联网网络安全和
			数据安全工作的通知 第十三条
检测机构	接受相关企业委托，开展网络安全符合性评测和风险评估	定期	关于加强车联网网络安全和数据安全工作的通知 第五条
安全评估的机构和人员	不得披露评估中获悉的汽车数据处理者商业秘密、未公开信息，不得将评估中获悉的信息用于评估以外目的	——	汽车数据安全管理若干规定 第十五条

检测评估机构负责开展网络安全符合性评测和风险评估，不得披露评估中获悉的运营者商业秘密、未公开信息，不得将评估中获悉的信息用于评估以外目的。

在向境外提供数据，赴境外上市，共享、交易、委托处理重要数据，利用个人信息进行自动化决策等情况下，将触发数据安全评估。

1、在向境外提供数据时，分为提供数据、个人信息、重要数据三类情形。

（1）提供数据的情形。国家机关要进行安全评估，可以要求有关部门提供支持与协助；关键信息基础设施运营者要通过国家网信部门组织的安全评估；数据处理者在符合国家网信部门规定的需要申报数据出境安全评估的情况下（具体情况在数据出境安全评估办法第四条中予以明确）要通过所在地省级网信部门向国家网信部门申报数据出境安全评估。

（2）提供个人信息的情形。国家网信部门负责组织数据出境安全评估。个人信息处理者进行个人信息保护影响评估，并对处理情况进行记录。其中，处理个人信息达到国家网信部门规定数量或者属于汽车行业的个人信息处理者，需要通过国家网信部门组织的数据出境安全评估。

（3）提供重要数据的情形。国家网信部门负责组织数据出境安全评估。重要数据处理者需要通过国家网信部门组织的数据出境安全评估。对于智能网联汽车生产企业和车联网服务平台运营企业，除了需要进行数据出境安全评估，还需要向所在省（区、市）通信管理局、工业和信息化主管部门报备。

2、在赴境外上市时，数据处理者要自行或者委托数据安全服务机构每年开展一次数据安全评估，每年 1 月 31 日前将上一年度数据安全评估报告报设区的市级网信部门，并至少保留三年的风险评估报告。

3、共享、交易、委托处理重要数据时，数据处理者要开展安全评估，评估认为可能危害国家安全、经济发展和公共利益的，不得共享、交易、委托处理重要数据。

4、涉及利用个人信息进行自动化决策的个人信息处理者，要进行个人信息保护影响评估，并对处理情况进

行记录。

（六）数据安全管理责任更加夯实，管理能力建设任重道远

明确专门的数据安全负责人和管理机构，是压实数据安全管理责任的重要基础。法律法规对达到国家网信部门规定数量的个人信息处理者、重要数据处理者，以及汽车数据处理者，均明确提出了设立数据安全负责人和管理机构的要求，为数据安全管理工作提供基础保障。但充分发挥数据安全管理责任，还需要借助先进的数据安全管理平台，支撑数据安全相关重大决策、数据安全事件应急响应、数据安全风险监测、数据安全风险和事件处置、数据安全风险评估，有效提升数据安全管理能力。

法律法规对国家机关、数据处理者（个人信息处理者、重要数据处理者、汽车数据处理者）、汽车行业相关企业在数据安全管理责任方面进行了明确。

国家机关重点负责建立健全数据安全管理制度的总体要求，落实数据安全保护责任，保障政务数据安全。

数据处理者的职责主要面向个人信息处理者、重要数据处理者、汽车数据处理者。

个人信息处理者在处理个人信息达到国家网信部门规定数量时，要指定个人信息保护负责人，公开个人信息保护负责人的联系方式，并将个人信息保护负责人的姓名、联系方式等报送履行个人信息保护职责的部门。

重要数据处理者要明确数据安全负责人，成立数据安全管理机构，研究提出数据安全相关重大决策建议，制定实施数据安全保护计划和数据安全事件应急预案，开展数据安全风险监测，及时处置数据安全风险和事件，定期组织开展数据安全宣传教育培训、风险评估、应急演练等活动，受理、处置数据安全投诉、举报，向网信部门和主管、监管部门报告数据安全情况。

汽车数据处理者在开展重要数据处理活动时，向省、自治区、直辖市网信部门和有关部门报送年度汽车数据安全管理情况（包括汽车数据安全管理负责人、用户权益事务联系人的姓名和联系方式）。

汽车行业相关企业要建立网络安全和数据安全管理制度，明确负责人和管理机构，落实网络安全和数据安全保护责任。

表 6 数据安全管理责任的主体及职责

主体	责任范围	时间要求	法律法规
国家机关	建立健全数据安全管理制度，落实数据安全保护责任，保障政务数据安全	——	数据安全法 第三十九条
个人信息处理者	处理个人信息达到国家网信部门规定数量时，指定个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督	——	个人信息保护法 第五十二条
	公开个人信息保护负责人的联系方式，并将个人信息保护负责人的姓名、联系方式等报送履行个人信息保护职责的部门	——	个人信息保护法 第五十二条
重要数据处理者	明确数据安全负责人和管理机构，落实数据安全保护责任	——	数据安全法 第七十二条（第二款）
	明确数据安全负责人，成立数据安全管理机构	——	网络数据安全管理条例 第二十八条
	研究提出数据安全相关重大决策建议	——	网络数据安全管理条例 第二十八条
	制定实施数据安全保护计划和数据安全事件应急预案	——	
	开展数据安全风险监测，及时处置数据安全风险和事件	——	
	定期组织开展数据安全宣传教育培训、风险评估、应急演练等活动	——	
	受理、处置数据安全投诉、举报	——	
	向网信部门和主管、监管部门报告数据安全情况		
汽车数据处理者	开展重要数据处理活动时，向省、自治区、直辖市网信部门和有关部门报送年度汽车数据安全管理情况（包括汽车数据安全管理负责人、用户权益事务联系人的姓名和联系方式）	每年十二月十五日前	汽车数据安全管理若干规定 第十三条（第一款）
各相关企业	建立网络安全和数据安全管理制度，明确负责人和管理机构，落实网络安全和数据安全保护责任	——	关于加强车联网网络安全和数据安全工作的通知 第一条

（七）数据安全培训要求显著提高，部分主体须开展强制学习

法律法规明确要求个人信息处理者要定期对从业人员进行安全教育和培训，重要数据处理者要每年组织开展全员数据安全教育培训，数据安全相关的技术和管理人员每年教育培训时间不得少于二十小时。这些刚性需求创造了巨大市场增量，加上国家在《数据安全法》《网络数据安全管理条例》中明确提出了鼓励支持数据开发利用技术和数据安全培训的政策，未来数据安全市场有望实现快速增长。

在数据安全培训方面，法律法规对国家、个人信息处理者、重要数据处理者、汽车行业相关企业的主要职责进行明确。

国家明确支持教育、科研机构和企业等开展数据开发利用技术和数据安全相关教育和培训，鼓励国家机关、行业组织、企业、教育和科研机构、有关专业机构等开展数据开发利用和安全保护合作，开展数据安全宣传教育和培训。

个人信息处理者要定期对从业人员进行安全教育和培训。

重要数据处理者要制定数据安全培训计划，每年组织开展全员数据安全教育培训，数据安全相关的技术和管理人员每年教育培训时间不得少于二十小时。

汽车行业相关企业要加强网络安全和数据安全宣传、教育和培训。

（八）数据安全审计地位更加提升，数据合规成为审计重点

相比美欧等国家地区，我国对数据安全领域的审计重视程度不够，运用不充分，除了银行业等重点行业（银保监会 2018 年发布《银行业金融机构数据治理指引》提出了定期审计数据安全的要求），数据安全审计尚未纳入公司年度业务管理的必要组成。

随着数据安全问题的加剧和地位的上升，在今年发布的数据安全法律法规中，对主管部门、监管部门、个人信息处理者、数据处理者、大型互联网平台运营者都提出了定期组织或开展数据安全审计、合规审计等要求，特别是大型互联网平台运营者，更是要求每年对平台数据安全情况、平台规则和自身承诺的执行情况、个人信息保护情况、数据开发利用情况等进行年度审计，并披露审计结果。未来，随着数字经济的快速发展，数据安全审计、合规审计将更加推广，成为国家监管、公司业务运营的重要方面。

在数据安全审计方面，明确了国家、主管部门、监管部门、个人信息处理者、数据处理者、大型互联网平台运营者的主要职责。

国家层面重点明确了建立数据安全审计制度的要求。

主管部门和监管部门负责组织开展对重要数据处理活动的审计，重点审计数据处理者履行法律、行政法规规定的义务等情况。

个人信息处理者应当定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。

数据处理者应当委托数据安全审计专业机构定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。

大型互联网平台运营者应当通过委托第三方审计方式，每年对平台数据安全情况、平台规则和自身承诺的执行情况、个人信息保护情况、数据开发利用情况等进行年度审计，并披露审计结果。

表 7 数据安全审计的主体及职责

主体	责任范围	相关对象	时间要求	法律条款
国家	建立数据安全审计制度	——	——	网络数据安全管理条例 第五十八条
主管部门监管部门	组织开展对重要数据处理活动的审计，重点审计数据处理者履行法律、行政法规规定的义务等情况	——	——	网络数据安全管理条例 第五十八条
个人信息处理者	对其处理个人信息遵守法律、行政法规的情况进行合规审计	——	定期	个人信息保护法 第五十四条
数据处理者	委托数据安全审计专业机构定期对其处理个人信息遵守法律、行政法规的情况进行合规审计	数据安全审计专业机构	定期	网络数据安全管理条例 第五十八条
大型互联网平台运营者	通过委托第三方审计方式，每年对平台数据安全情况、平台规则和自身承诺的执行情况、个人信息保护情况、数据开发利用情况等进行年度审计，并披露审计结果	第三方审计机构	每年	网络数据安全管理条例 第五十三条

在发现个人信息处理活动存在较大风险或者发生个人信息安全事件时，履行个人信息保护职责的部门可以通过两种方式履行监管职责：一是对该个人信息处理者的法定代表人或主要负责人进行约谈，或者要求个人信息处理者委托专业机构对其个人信息处理活动进行合规审计。二是个人信息处理者需要按照要求采取措施，进行整改，消除隐患。

表 8 数据安全审计的触发条件及处理流程

触发条件	主体	责任范围	法律条款
发现个人信息处理活动存在较大风险或者发生个人信息安全事件时	履行个人信息保护职责的部门	对该个人信息处理者的法定代表人或者主要负责人进行约谈，或者要求个人信息处理者委托专业机构对其个人信息处理活动进行合规审计	个人信息保护法 第六十四条
	个人信息处理者	按照要求采取措施，进行整改，消除隐患	个人信息保护法 第六十四条

三、启示及建议

（一）针对数据处理者的建议

数据处理者主要涉及数据处理者、重要数据处理者、个人信息处理者、汽车数据处理者等四类主体。

1、数据处理者均需要重点关注数据安全应急处置和数据安全审计工作。建立数据安全应急处置机制；委托数据安全审计专业机构定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。

2、重要数据处理者需要重点关注数据安全评估、数据安全管理责任、数据安全培训等三项工作。(1) 数据安全评估方面，需要对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告。(2) 数据安全管理责任方面，一是明确数据安全负责人，成立数据安全管理机构；二是研究提出数据安全相关重大决策建议；三是制定实施数据安全保护计划和数据安全事件应急预案；四是开展数据安全风险监测，及时处置数据安全风险和事件；五是定期组织开展数据安全宣传教育培训、风险评估、应急演练等活动；六是受理、处置数据安全投诉、举报；七是向网信部门和主管、监管部门报告数据安全情况。(3) 数据安全培训方面，制定数据安全培训计划，每年组织开展全员数据安全教育培训；确保数据安全相关的技术和管理人员每年教育培训时间不得少于二十小时。

3、个人信息处理者需要重点关注分类分级保护、数据安全管理责任、数据安全培训、数据安全审计等四项工作。(1) 分类分级保护方面，需要对个人信息实行分类管理。(2) 数据安全管理责任方面，一是在处理个人信息达到国家网信部门规定数量时，要指定个人信息保护负责人，负责对个人信息处理活动及采取的保护措施等进行监督；二是公开个人信息保护负责人的联系方式，并将个人信息保护负责人的姓名、联系方式等报送履行个人信息保护职责的部门。(3) 数据安全培训方面，要定期对从业人员进行安全教育和培训。(4) 数据安全审计方面，要对其处理个人信息遵守法律、行政法规的情况进行合规审计。

4、汽车数据处理者需要重点关注数据安全管理责任，要向省、自治区、直辖市网信部门和有关部门报送年度汽车数据安全管理情况（包括汽车数据安全管理负责人、用户权益事务联系人的姓名和联系方式）。

（二）针对相关企业的建议

相关企业主要涉及大型互联网平台运营者、智能网联汽车生产企业、车联网服务平台运营企业、汽车行业相关企业等四类主体。

1、大型互联网平台运营者需要重点关注数据安全审计。要通过委托第三方审计方式，每年对平台数据安全情况、平台规则和自身承诺的执行情况、个人信息保护情况、数据开发利用情况等进行年度审计，并披露审计结果。

2、智能网联汽车企业和车联网服务平台运营企业需要重点关注分类分级保护、数据安全应急处置、数据安全评估等三项工作。（1）分类分级保护方面，要建立数据管理台账，实施数据分类分级管理，加强个人信息与重要数据保护。（2）数据安全应急处置方面，要建立网络安全应急响应机制，制定网络安全事件应急预案，定期开展应急演练，及时处置安全威胁、网络攻击、网络侵入等网络安全风险。(3) 数据安全评估方面，要开展数据安全风险评估，并向所在省（区、市）通信管理局、工业和信息化主管部门报备。同时，智能网联汽车企业还要加强在线升级服务（OTA）安全和漏洞检测评估；车联网服务平台运营企业在认定为关键信息基础设施时，还要自行或者委托商用密码检测机构开展商用密码应用安全性评估。

3、汽车行业相关企业要重点关注分类分级保护、数据安全评估、数据安全管理责任、数据安全培训等四项工作。(1) 分类分级保护方面，要严格落实网络安全分级防护要求，加强网络设施和网络系统资产管理，合理划分网络安全域，加强访问控制管理，做好网络边界安全防护。(2) 数据安全评估方面，要自行或者委托检测机构定期开展网络安全符合性评测和风险评估，及时消除风险隐患。(3) 数据安全管理责任方面，要建立网络安全和数据安全管理制度，明确负责人和管理机构，落实网络安全和数据安全保护责任。(4) 数据安全培训方面，要加强网络安全和数据安全宣传、教育和培训。

政策解读

加强政企协同，共同维护国家关键信息基础设施安全

作者 战略推进中心

习近平总书记在“4·19”重要讲话中明确指出：“关键信息基础设施是经济社会运行的神经中枢，是网络安全的重中之重，也是可能遭到重点攻击的目标。”当前国际社会风云变幻，网络安全风险层出不穷，关键信息基础设施（以下简称“关基”）安全保护工作的重要性和紧迫性日益凸显。党的十八大以来，国家高度重视网络安全工作。2021年9月1日，国务院颁布出台的《关键信息基础设施安全保护条例》（以下简称《条例》）正式实施，这是我国首部专门针对关基安全保护工作的行政法规，是加强网络安全工作的又一有力举措，开启了新篇章。

一、《条例》是新时期指导做好关基保护工作的纲领性文件

近几年，全球范围内针对关基的供应链攻击、勒索攻击等安全事件日益增多，引起世界各国的重点关注。关基安全保护已上升到维护国家安全的高度。以美国为例，近十年陆续发布了一系列关键基础设施的保护计划和框架，指导政府、私营机构等各方共同做好关基安全保护工作。

党中央、国务院高度重视关基安全保护工作，习近平总书记明确提出：“必须深入研究，采取有效措施，切实做好国家关键信息基础设施安全防护”“要落实关键信息基础设施防护责任，行业、企业作为关键信息基础设施运营者承担主体防护责任，主管部门履行好监管责任”。《条例》的出台旨在落实习近平总书记重要指示精神，明确我国关基安全保护工作相关各方的职责要求和法律责任。《条例》是我国关基安全保护领域的纲领性文件，有助于构建多方尽责、共同协作的关基立体安全防护体系，更好地应对网络安全风险挑战。

二、《条例》承上启下进一步完善了我国网络安全法规体系

《网络安全法》是本条例的上位法，《条例》对《网络安全法》所确立的关基安全保护制度做了进一步细化完善，明确了国家网信部门、国务院公安部门及重要行业和领域的主管部门、监督管理部门（以下简称“保护工作部门”）等相关职能部门的责任边界和职责要求，明确了关基认定原则和认定机制，细化了运营者的主体责任和义务，形成了关基安全保护工作相关各方的法律责任体系。

各相关主管部门已经开展的涉及关基安全保护的相关工作，需要在本条例的要求框架下开展。重要行业和领域的主管部门还需要依据本条例制定本行业领域的关基安全保护和监督管理相关工作要求。

三、五大举措构建了关基网络安全政企协同的工作体系

（一）突出了统筹协调

《条例》第三条要求在国家网信部门统筹协调下，国务院公安部门负责指导监督关基安全保护工作。国务院电信主管部门、其他有关部门、省级人民政府有关部门依照本条例和有关法律、行政法规的规定，在各自职

责范围内负责关基安全保护和监督管理工作。此外，还明确了国家网信部门负责建立网络安全信息共享机制（第二十三条）、对关基进行网络安全检查检测（第二十七条）、为关基安全保护工作提供技术支持和协作（第二十九条）等。

鉴于网信部门的职责，《条例》的安排凸显了三方面考虑：一是统筹好关基建设与安全的关系；二是统筹好部门的工作；三是统筹好安全与创新的协同。

（二）明确了部门权责

在关基认定机制方面，本条例第二条对关基的定义和范围延续了《网络安全法》第三十一条的说法，并在第二章专门明确了关基的认定机制。《条例》第九条明确由保护工作部门制定本行业领域的关基认定规则，并从重要程度、危害程度和关联性影响三方面给出了三条考虑因素。保护工作部门负责组织认定本行业领域的关基，并将结果通报国务院公安部门（第十条）。如果关基发生较大变化可能影响认定结果的，保护工作部门需组织重新认定，结果通知运营单位并通报国务院公安部门（第十一条）。

在行业监管方面，《条例》明确各保护工作部门负责本行业领域的关基安全保护相关工作，包括制定安全规划（第二十二条）、建立健全监测预警制度（第二十四条）、建立应急预案、组织应急演练（第二十五条）、检查检测（第二十六条）等。

（三）强化了主体责任

《网络安全法》第三十三条至第三十八条对关基的

运营者责任提出了相关要求，《条例》在此基础上做了进一步补充完善，特别强调了关基运营者（以下简称“运营者”）要落实主体责任（第四条），对运营者提出了更全面细化的责任要求。包括在网络安全等级保护基础上采取保护措施（第六条），安全保护措施与关基三同步原则（第十二条），建立健全网络安全保护制度和责任制、保障人财物投入、明确运营者的主要负责人负总责（第十三条），设置专门安全管理机构并对相关人员进行安全背景审查（第十四条），明确专门安全管理机构的八条具体职责（第十五条），保障专门管理机构运行经费、人员配备和参与网络安全和信息化有关决策（第十六条），每年至少进行一次网络安全检测和风险评估（第十七条），遇到重大或特别重大的网络安全事件和威胁时履行报告制度（第十八条），采购网络产品和服务的原则和进行安全审查的情形（第十九条），要求并监督产品和服务提供者履行保密义务和责任（第二十条），发生合并、分立、解散等情况的工作要求（第二十一条）。

通过上述规定，细化明确了运营者的责任义务要求，从责任体系、制度建设、人员管理、能力建设、运行维护、供应链管理等方面指导运营者建立健全关基安全保障体系。

（四）规范了行为管控

关于禁止行为，《条例》明确要求任何个人和组织不得实施非法侵入、干扰、破坏关基的活动，不得危害关基安全（第五条），未经国家网信部门、国务院公安部门批准或者保护工作部门、运营者授权，任何个人和组织不得对关基实施漏洞探测、渗透性测试等活动，对基础电信网络实施漏洞探测、渗透性测试等活动，应事先向国务院电信主管部门报告（第三十一条），公安机关和国家安全机关负责防范打击相关违法犯罪活动（第三十三条）。

（五）加强了生态建设

为加强国家关基安全保护生态体系建设，《条例》还对关基安全标准制定（第三十四条）、人才队伍建设（第三十五条）、技术创新和产业发展（第三十六条）、服务机构建设和管理（第三十七条）、军民融合和军地合作（第三十八条）等做了原则性要求，此外《条例》第三十二条还特别规定了能源、电信等关基的优先保障原则。

四、落实《条例》是各级政府和企业共同的责任

2022 年是党的二十大召开的政治之年，是实施“十四五”规划的深化之年，更是关基安全建设规划和实施的关键年，立足新时期，面向新要求，各级政府和企业应当严格按照《条例》要求切实履行主体责任，建立健全内部网络安全制度体系，强化以能力为导向的安全防护体系建设。

一是要建立切实可操作的政企协同联动机制。加强政府与企业之间网络安全信息、资源的共享，推动政府的安全基础设施向网络安全企业开放，鼓励安全企业赋能关基的安全建设，加快建立保护关基网络安全的政产学研用生态体系。

二是以新一代网络安全框架指导关基网络安全体系建设。以内生安全理念为指导，以系统工程方法改变过去局部整改、辅助配套的建设模式。“十四五”时期的网络安全建设，每一个任务设置都要将管理、技术、运行等各方面的要素综合考虑，避免割裂。各任务之间相互关联、能力互补，形成有机的整体，具备体系化作战的能力。

三是强化网络安全与信息化的融合发展。实现安全规划、建设、运营与信息化建设的全周期同步开展，安全能力要对信息化全面覆盖融合，安全成为信息化业务的内在属性。伴随信息化水平的持续升级，整体安全能力实现同步阶梯式上升。

四是建立安全运营体系与评估优化体系。安全运营体系全面涵盖安全团队、安全运行流程、安全操作规程、安全运行支撑平台和安全工具等。建立面向效果而非过程的评价体系，并以数据分析的方式对整改优化提供支撑，以数据分析结果牵引新安全建设工作，持续提升网络安全工作成熟度。

合规实践

平均泄露成本高达 435 万美元 数据安全合规该怎么搞?

作者 虎符智库研究员 魏开元

2016 年，Uber 遭黑客攻击导致大量用户信息失窃，事件曝光后的 2018 年，Uber 违反州数据泄露通告法律被罚 1.48 亿美元；

2018 年，因多达 5 亿客户的信息被泄，万豪国际也被 ICO 处以了 1.24 亿美元的罚款；

2022 年，爱尔兰数据保护委员向 Instagram 开出了 4 亿美元的天价罚单，原因是该公司默认将 13 岁至 17 岁儿童的账户设置为公开状态，并允许拥有商业账户的青少年公开自己的电子邮件地址和电话号码；

……

随着国内外数据安全相关法律法规的逐步完善，因违反相关规定导致重大数据泄露事件而被处以顶格罚款的新闻，早已是屡见不鲜。在近期公开的《关于修改〈中华人民共和国网络安全法〉的决定（征求意见稿）》中，也将重大违法事件的罚款上限大幅提高到了五千万元或者年营收的 5%。

除罚款外，因数据泄露而带来的直接经济损失也呈现出不断上涨的趋势。

根据 IBM 最新发布的《2022 年数据泄露成本报告》，数据泄露的平均成本创下 435 万美元的历史新高，比 2021 年增长了 2.6%，自 2020 年以来增长了 12.7%。而且今年的研究首次发现，83%受访组织已经不是第一次发生数据泄露事件。

显而易见的是，数据安全风险正在使得机构“钱袋子”的压力陡然增加。

被忽视的风险——特权

《数据安全法》第二十九条明确规定，开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施。

当然，数据安全风险多种多样。

根据国际权威机构 Verizon 发布的《2022 年数据泄露调查报告》显示，目前有凭证窃取、网络钓鱼、漏洞利用和僵尸网络等四个主要途径会威胁到数据资产。

为此，企业不得不采取多种检测和防御手段，试图阻止攻击者入侵的脚步。

不过，出于多种原因，部分安全措施并没有达到预期的效果，数据泄露依然持续发生。IBM 调查发现，83%受访组织已经不是第一次发生数据泄露事件。

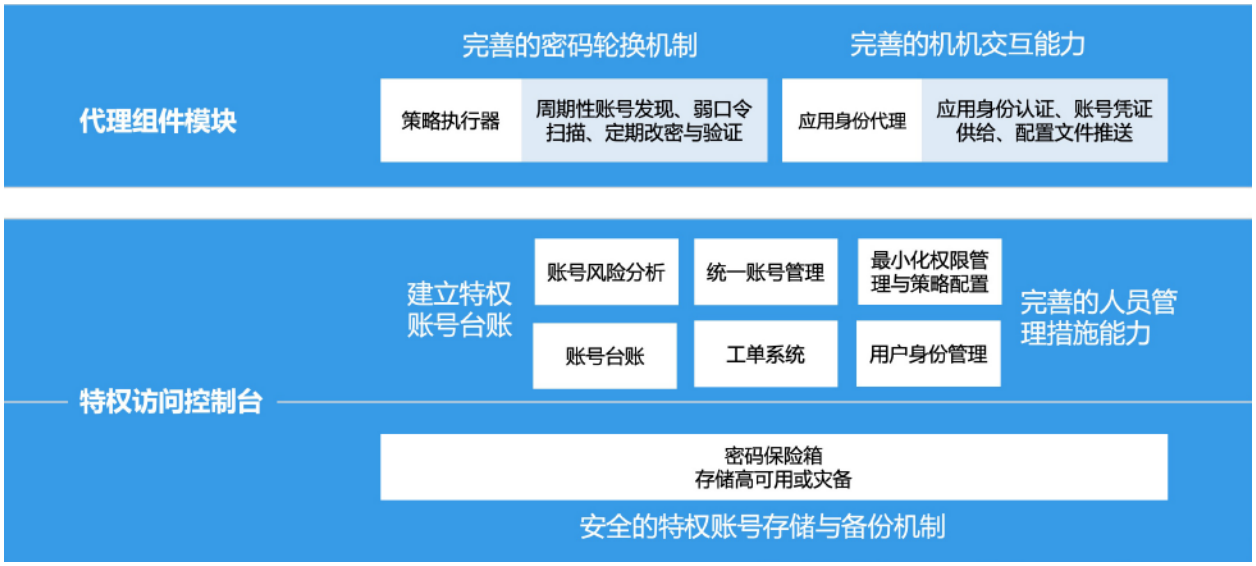
特别的是，在 Verizon 分析的 23896 个安全事件中，82% 的违规事件涉及人为因素，近一半的数据泄露事件，与特权账号的登录凭证丢失有直接关系。无论是凭证丢失、网络钓鱼、误用等简单的错误，人在安全事件和数据漏洞事件中始终扮演着非常重要的角色。

而人的背后，则是访问企业核心数据的特权——无论攻击者或者内部的恶意人员采用怎样的攻击手段、无论是攻击 API 还是数据库以达到窃取数据的目的，其首要目标都是为了获取较高的访问权限。

比如，在奇安盘古披露的美国针对全球的网络窃密事件“电幕行动”中，NSA 便利用“饮茶”嗅探木马窃取目标系统内多个进程中的账号密码，用于实施下一步的攻击行动。

奇安信集团数据安全子公司副总经理姚磊认为，无论是抵挡外部攻击者还是防范内鬼，保障数据安全合规、做好风险管控的第一步核心是管理好特权账号，因为特权账号是通往企业数据大门的“钥匙”，最容易成为突破口。

不过相比于入侵检测、防火墙等耳熟能详的网络安全手段，特权账号的安全是最容易被忽视也是最难做好



的。

特权管理的五大“硬伤”

很多人会发出疑问，离职了尽快冻结账号，密码及时更换，不就解决泄密问题了？但事情远没有那么简单。姚磊认为，弱密码、幽灵账号、僵尸账号、提权账号等风险账号屡禁不止的背后，一定是符合了某些人性和管理的硬伤。

第一是人的趋利性。“天下熙熙，皆为利来；天下攘攘，皆为利往。”在利益趋势下，总有内鬼不断出现，内部泄密手段防不胜防。而网络犯罪日益猖狂，不法分子无利不起早，新型手段往往能找到最薄弱的一环。

第二是账号的天然分散性。随着业务增长，管理资源的增多，各种账号动辄上万，分布在主机、网络设备、数据库等资产上，非常分散，难以全面梳理，做不到心中有数。

以思科前程序员“删虚拟机跑路”的事件为例，后端服务器资源上的账号变化无法有效追踪，比如，开发运维人员私自创建的账号、提权的账号、长期不登录的僵尸账号、外包人员申请的临时账号等，由于缺乏行之有效的管理工具，极易造成账号泄露。

第三是人管理的惰性，弱密码使用的方便性、记忆的便捷性、管理的统一性，说明了由人脑设置和管理密码必会导致弱密码的产生。之前媒体报道，乌克兰武装部队某重要系统使用弱口令，账号是 admin，密码是 123456，引发业内哗然。重要数据资产环境存在的弱口令问题，会使攻击门槛大幅降低，黑客可以通过暴力破解或其他方法轻易攻破核心资产的“大门”，对数据安全造成极大威胁。

第四是人管理的疏忽性。特权账号使用流程难闭环、密码记不住，存储不安全。之前有不少明文存储账号的报道，如明文存储在 Excel 表格、笔记本或文本中，一

旦终端失陷，将造成大批核心主机或数据库失陷，极具安全隐患。

第五是机器规则和人工管理的天然矛盾。 平台规则不一样，改密难统一、系统内嵌无法改，费时费力且没效果。

三大“锦囊”给企业数据加上层层“保护锁”

姚磊总结到，网络安全建设的好坏往往是木桶效应，取决于最薄弱的一环；而特权账号则是直接关系到企业数据安全，往往是内外风险最集中突破的大门。为了保护好这扇大门，姚磊给出了三个“锦囊妙计”。

锦囊 1 号——风险可视 建立台账

为防止账号被盗，应当采用专业的安全工具建立特权账号台账。通过台账定期扫描系统账号，发现高风险账号及其分布情况，消除并持续监测账号风险动态；实施系统弱密码扫描专项，录入企业内部专属的弱密码集合，并且一键改密，防止利用相同口令的内网横向移动；综合分析账号活动、账号会话、风险账号情况，识别可疑行为和检测正在进行的攻击，管理人员可以通过梳理的特权账号台账对高风险账号与行为进行快速治理。

锦囊 2 号——“往来有序，完善机制”

姚磊认为，在员工流动成为常态的情况下，往来有序，完善人员管理机制至关重要。企业应当通过统一管理平台一键收回员工账号权限，完善人员管理机制，及时清除过期、多余的账号，避免离职或调岗人员非法访问，落地最小权限管理原则。

同时，人员管理应根据工作需要，在有限时段内授予用户对特定系统、应用程序或目标设备的访问权限，避免特权账号的长期持有，并采取细粒度的命令控制策略，阻断权限升级及滥用，降低内部人员非法利用特权账号造成数据泄漏或系统破坏的风险。

锦囊 3 号——“运筹帷幄，闭环管理”

为了避免僵尸账号、临时账号长期存在，成为“定时炸弹”，姚磊建议建立特权账号的全生命周期管控机制。它覆盖账号生成、属性变更、账号存储、账号使用、口令轮换、账号销毁等特权账号生命周期的各个环节，确保账号安全可知、可管、可控、可查。针对各类账号，应当通过制定完善的改密策略，定期自动地下发账号改密命令，批量地修改特权账号口令，消除风险账号。以及建立特权账号存储的高安全性、高可用性及灾备能力，完善的账号口令备份机制，牢牢保护账号安全。

综上所述，姚磊给出了解决特权账号难题的终极大招——特权账号安全方案。他认为，特权账号、密码的管理不是靠人力和制度能做好的事情，而特权账号安全方案，可以无忧解决特权账号的管理问题和安全挑战。

总而言之，特权账号安全方案是利用设备去做特权账号全生命流程的管理，以及高安全性密码存储方案，即可帮助广大数字化转型中的政企客户消除数据泄密的风险，应对内鬼泄密、外部入侵等安全挑战。

同时，针对国内企业机构的数据的安全现状，奇安信发布了包括特权账号安全在内的保障数据安全的“五件套”，即特权账号管理、堡垒机、数据库审计、API 安全卫士和数据安全态势感知，能够帮助政企机构在数据安全建设过程中的“补短板、防裸奔”期间，进行全方位多维度的数据安全保障，帮助企业兼顾业务发展和安全合规。

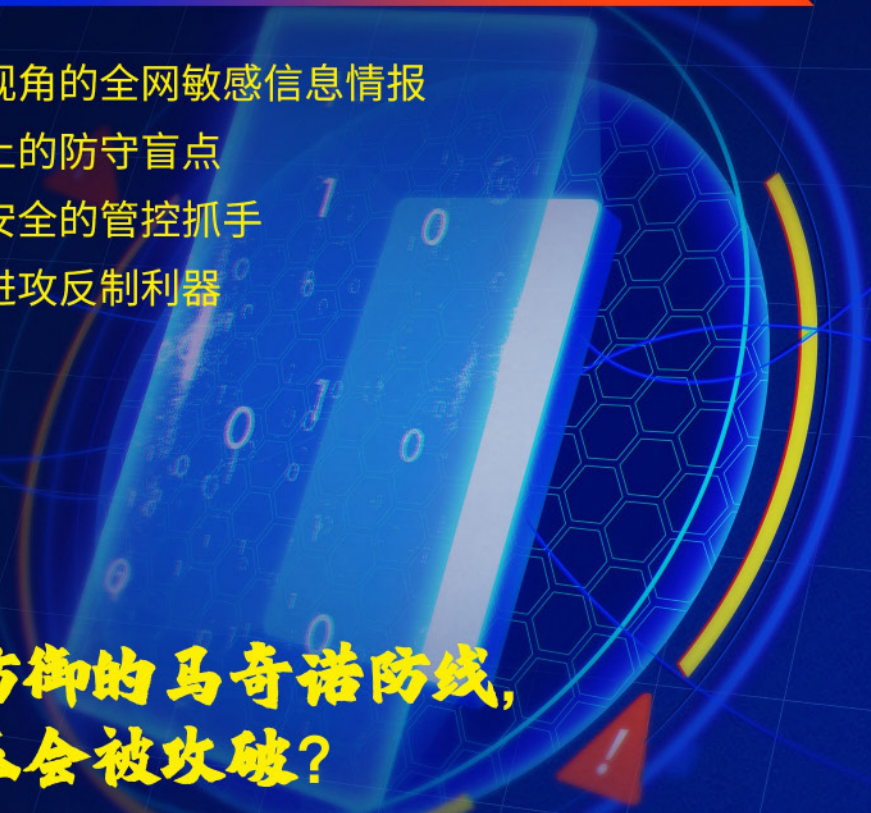
今年 7 月，奇安信旗下多款数据安全产品，全部通过了中国信通院在开展的七大品类的测评认证，成为首家获得全套数据安全产品测评资质证书的网络安全企业。

大数据环境下，业务系统和数据流转比较复杂，传统数据安全防护理念和方法已经难以胜任，需要数据安全管理和技术的融合，从组织、制度、流程上完善数据安全管理体系，这样才能有效的支撑数据安全合规更好的落地执行。

奇安信

敏感信息泄露情报服务

- 攻击队视角的全网敏感信息情报
- 急需补上的防守盲点
- 供应链安全的管控抓手
- 预防性进攻反制利器



纵深防御的马奇诺防线，为什么会被攻破？

- 完整的防御体系，既要考虑正面防御，侧翼的情报收集和对抗也必不可少！
- 忽视全网视角的情报，是防守的重大盲点！

服务定位 SERVICE POSITIONING

- **攻击队视角**：使用渗透专家交付，不是简单的信息收集。
- **全网视角**：核心功能是从外部探测全互联网第三方应用中的敏感泄露数据；而非只关心自己的网络和应用。
- **情报级**：专家梳理的情报级信息，而不是简单数据抓取：给出利用思路和可能的攻击链，更有详细的整改建议。

奇安信安服团队

合规实践

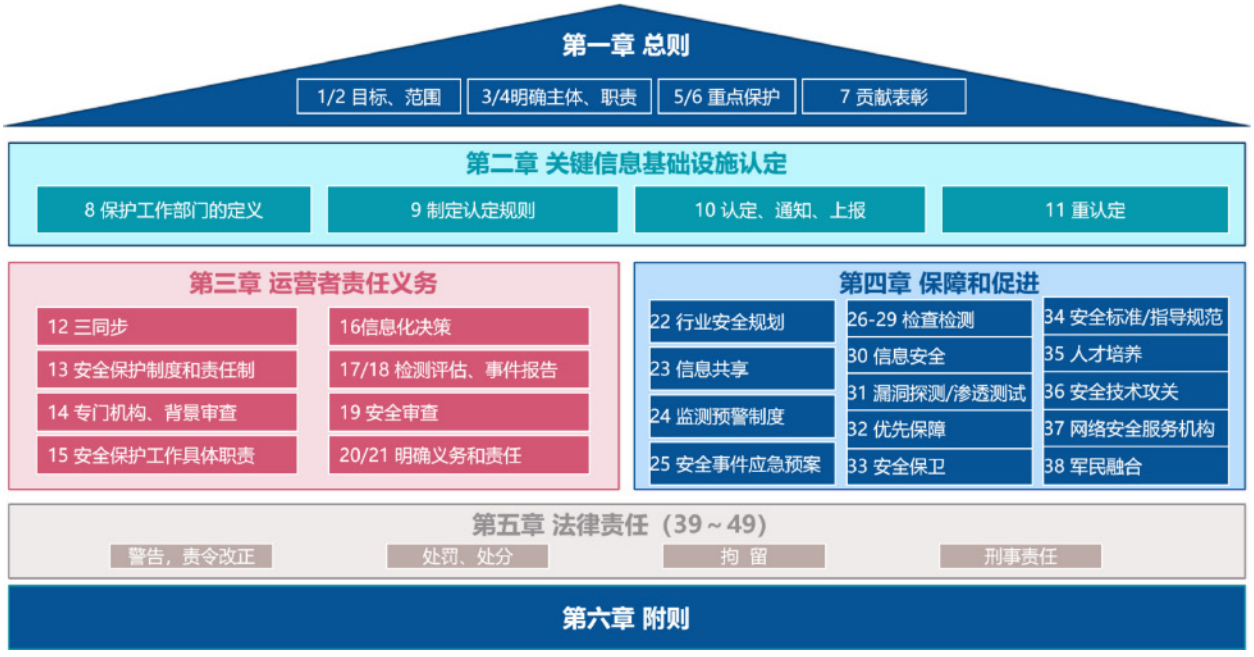
新合规时代 《关保条例》实施需兼顾合规性和有效性

作者 解决方案中心 钟君毅

2021 年，可以称之为网络安全的“觉醒年代”。这一年，《关键信息基础设施安全保护条例》（简称《条例》）、《数据安全法》、《个人信息保护法》陆续施行，网络安全走向新合规时代，在合规的基础上更多地关注有效性，切实地保障关键信息基础设施安全稳定的运行。

2022 年，可以称之为网络安全新合规的落地实施年，各项指导细则、管理办法等持续推出。针对关基保护，很多行业（如电力、交通、卫生等）结合关键信息基础设施安全保要求发布了本行业的网络安全管理办法。从国家层面来看，依照时间顺序分别是 2022 年 2 月 15 日起施行的修订后的《网络安全审查办法》、2022 年 6 月 23 日发布的《国务院关于加强数字政府建设的指导意见》（国发〔2022〕14 号）和 2022 年 9 月 12 日的面相社会征求意见的《中华人民共和国网络安全法》的征求意见稿。

以《条例》为例，它以问题为导向，针对网络安全保护中突出的问题，细化《中华人民共和国网络安全法》的有关规定，将实践证明成熟有效的做法上升为法律制度，同时关键信息基础设施安全保护坚持综合协调、分工责任、依法保护，强化和落实关键信息基础设施运营者主体责任，充分发挥政府及社会各方面的作用，共同



图：《关保条例》总体框架

保护关键信息基础设施安全。该条例的实施，对于维护国家网络空间主权和国家安全、保障经济社会健康发展、维护公民合法权益，具有重大意义。

条例持续细化 对推动行业合规落地效果显著

整个 2022 年，在网络安全相关法律法规完善建设方面，最显著的特色，就是不断强化安全保护责任，明确和细化安全审查具体要求，为加速行业合规落地提供良好的政策法规基础。

在关基保护中，根据《 条例 》第十九条，运营者应当优先采购安全可信的网络产品和服务；采购网络产品和服务可能影响国家安全的，应当按照国家网络安全规定通过安全审查。网络安全审查办法明确和细化了网络安全审查的具体要求，为关键信息基础设施运营者申报审查提供了指引。

而在《 国务院关于加强数字政府建设的指导意见 》中，从强化安全管理责任、落实安全制度要求、提升安全保障能力、提高自主可控水平四个方面进行阐述，从而构建数字政府全方位安全保障体系，切实筑牢数字政府建设的安全防线。

同样，在《 网络安全法 》的征求意见稿中，为强化关键信息基础设施安全保护责任，进一步完善关键信息基础设施运营者有关违法行为行政处罚的规定，为下一步动作奠定了基础。

《条例》落地需兼顾合规性和有效性

从 2021 年到现在，密集出台的法律法规，显著激发了客户对网络安全合规的需求。例如，《 数据安全法 》颁布后，明显数据安全的合规需求旺盛起来，《 条例 》》实施后，对关基相关重要行业和领域的影响面也非常显著。

在关保条例施行前，国内遵循最多的就是等保相关的制度进行建设，等保的前身是基于美国 IATF 信息保障技术框架出来的，它是建立在信息基础设施概念上的，倡导“一个中心三重防护”。在国家提出“数字强国”战略、各行业推进数字化转型的环境下，安全的本质是要解决业务连续性和安全风险相关的问题，脱离业务就很难让安全达到很好的效果，因此关保更多是从业务视角出发，面向业务的安全治理。这一点从《 条例 》中“运营者责任义务”的第一条就能看出，其中提到，“安全保护措施应当与关键信息基础设施同步规划、同步建设、同步使用。”同样，奇安信坚信实施三同步是使得安全与业务融合，实现内生安全最重要的保障机制。

由此来看，与《 条例 》配套的关键信息基础设施安全保护要求（ 报批稿 ）里面重点讲的是安全防护前的业务、资产的分析识别，做安全检查和风险评估，以及安全防护后的监测预警和事件处置，本质上是把关注安全的建设过程牵引到关注业务的结果导向，所以，这也就有了合规性和有效性的说法，即关基运营者在网络安全建设中，合规性和有效性需两者兼顾，不可分割。

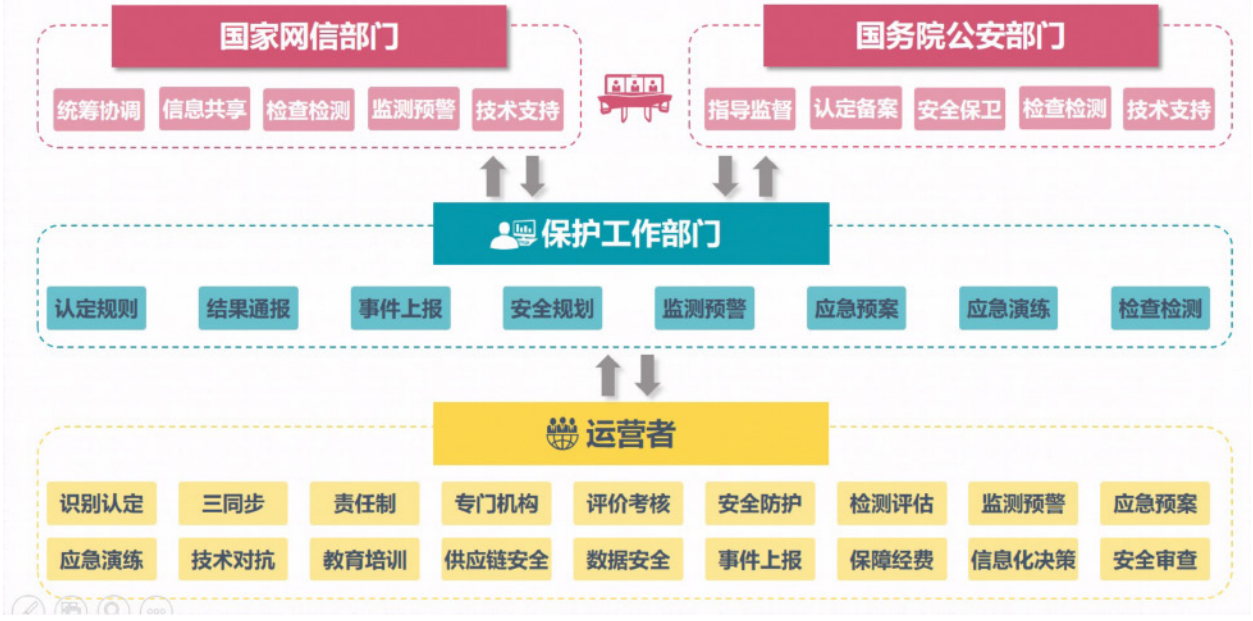
然而，由于《 条例 》仅发布一年多，从实战角度，合规性和有效性依然是《 条例 》落地的两大难点。

第一是合规性的细则有待进一步清晰。

自关保条例正式施行之后，网信部门有相关指导意见，公安也下发了相关重点措施，旨在指导关基保护的相关建设，同时关键信息基础设施安全保护要求（ 报批稿 ）已经处于报批稿待发状态，从法律法规、相关标准及监管机构的发文，在现阶段已经能够做到有法可依、有法必依，但是在具体的执行层面、比如安全检查要如何开展、安全规划要如何落到实处、相关的流程规范及参考的细化标准都有哪些，这些内容还有待进一步的清晰。

第二是有效性需更深入和全面的评估考量。

正如前文所说，安全的本质是要解决业务和安全风险相关的问题，脱离业务就很难让安全达到很好的效果。



图：《关保条例》实施相关部门和组织

因此，关基保护更多地是从业务视角出发，基于动态风控的思路，实现面向业务风险的安全治理。不同行业、不同领域的关基保护部门与运营者要如何根据自身的网络安全风险去开展相应的体系化建设，要做到什么地步才算满足关基保护的要求，这一部分的内容在未发布的关键信息基础设施安全防护能力评价方法有部分提及，后续是否调整、调整的范围多大，以及具体什么时间发布，现在还不太清楚。

在这个过程中，关基运营者普遍会产生大量安全服务的需求，通过安全服务（如安全检查、风险评估、攻防演习）来检验安全能力是特别有效的方式，不断提升安全保护能力和对抗能力，安全检查主要是查找关键信息基础设施存在的漏洞和安全隐患，风险评估则是以业务、资产的维度结合威胁、脆弱性的情况去定义相关的风险，攻防演习则是通过实战的方式去评估关键安全防护的短板。

作为国内领先的网络安全公司，奇安信的安服团队积累了非常丰厚的经验。从 2018、2019 年开始，奇安信安服就成立了专门的团队，专职对国家的关基保护体系进行探究，也进行了一些行业的“实验局”建设。所有这些努力，推动了多个客户从最初的工作任务规划到关基的认定规则，再到保护指南、规划的编制，最后到具体的项目落地（调研、评估等），都是全程参与并且是主导地位，整体取得了很好的效果。

四大举措破解难点，加速《条例》落地执行。

目前，在《条例》的指引下，关基保护在需要开展的工作方向上，已经相对比较清晰，然而在具体的执行层面，还没有太细化的标准。奇安信认为，关基单位可以在以下四个方面加快《条例》的落地和实施。

首先，在安全管理体系方面，需要明确关键信息基础设施的领导体系和工作体系，设置专门安全管理机构，建立领导机构决策机制，明确责任清单，加强制度流程建设及专业人才队伍建设，从实战出发制定并落实标准化文件，通过安全技术控制点落实安全管理要求，通过流程规范固化、落实安全工作和安全技术控制点，形成

图：《关保条例》具体行动总体框架

闭环与团队协同。

其次，在安全保障体系方面，开展安全检查风险评估，制定应急预案，组织开展应急演练工作，同时针对发现的安全威胁和发生的安全事件，开展服务保障和运行支撑相关的工作，保证闭环管理。

再次，在技术防护体系方面，需深入实施网络安全等级保护制度，在此基础上开展国产密码应用改造并推进国产化产品替代，强化供应链安全管理和数据安全治理防护，并根据安全检查风险评估的结果，针对性地进行整改加固，持续收敛暴露面。

最后，在技术防护体系的低位防御能力之上，依托中位的安全监控和高位的威胁情报能力，构建网络安全监控指挥中心，针对高级威胁进行监测发现攻击者，针对威胁事件进行分析研判处置并及时预警，提升安全数据支撑能力、威胁检测分析能力、联动响应处置能力、安全事件溯源能力、风险监测预警能力，提升持续安全运营能力，抵御大规模有组织网络攻击，有效维护关键信息基础设施安全。

总体来看，关基运营者合规建设一方面是遵纪守法的范畴，要做到有法可依，有法必依，执法必严，违法必究，守住合规红线；另一方面就是关基保护提到的重点保护，必须要从实战角度出发，立足有效性来开展网络安全建设，在安全的前提下，确保业务连续性和可靠性。

结束语：

在当前国际严峻的威胁形势下，我国的政企机构清晰地认识到网空范围下的强敌环视形势没有变，敌强我弱的形势没有变，“卡脖子”问题没有变，进行关键信息基础设施安全保护任务是重中之重。因此，网络安全工作迫切需要体系化的建设，特别是关键信息基础设保护工作涉及到国家指导、行业保护、网络服务机构、运营者落实等多方协同，筑牢网络安全底板，才能落实《条例》要求，化解重大风险，保障业务正常运转，为我国数字强国之路保驾护航。安

合规实践

筑牢网络安全基石！密评大考如何顺利“过关”？

“现行的《密码法》对有关违法行为的最高处罚为100万，其力度相较于现行《个人信息保护法》及前不久公布的《关于修改〈中华人民共和国网络安全法〉的决定（征求意见稿）》都小。”奇安信密码安全专家表示，随着网络安全违法行为处罚力度的不断加大，不排除未来在密码领域处罚力度上“加码”的可能。

密评成为商用密码合规的关键大考

商用密码应用安全性评估（简称“密评”），是指在采用商用密码技术、产品和服务集成建设的网络和信息系统中，对其密码应用的合规性、正确性和有效性进行评估。其目的是在信息系统中使用国产商用密码算法以实现对于信息系统中关键数据在终端、存储、传输、设备等层面的自主可控的安全防护。

密评的测评对象是信息系统。所使用的商用密码为国产密码算法的一类，包括对称密钥算法、非对称密钥算法、哈希算法及密钥交换算法等。对于合规性和正确性的要求，包括密码算法、密码协议、密钥管理、密码产品和服务的使用依照《商用密码管理条例》及GB/T 39786-2021《信息系统密码应用基本要求》；对于有效性则要求商用密码的使用、设计合理能够发挥效用，保障信息的机密性、完整性、真实性及不可否认性。

可以看到，密评已成为国家法律、法规强制要求的一项测评，成为相关机构不得不通过的一场大考。

实际上，我国针对密码的管理规范由来已久。早在1999年10月，我国就出台了《商用密码管理条例》，彰显了我国从密码层面对信息系统数据防护的重视。接着《信息安全等级保护商用密码管理办法实施意见》《网络安全法》《关键信息基础设施安全保护条例》《政务信息系统政府采购管理暂行办法》《网络安全等级保护条例》、《信息系统密码应用基本要求》，以及《国家政务信息化项目建设管理办法》相继出台，从政策层面相继指导是否要使用国产商用密码对业务系统进行防护、什么系统需要使用商用密码进行防护、如何使用商用密码进行密码防护、不采用商用密码保护信息有何后果（限制建设、暂停项目等）。

除此之外，各部门也相继出台了相关规范。

中共中央办公厅、国务院办公厅发布的《金融和重要领域密码应用与创新发展工作规划（2018-2022年）》要求构建以密码技术为核心的新网络安全体系，形成以密码基础设施为支撑的新网络安全环境。

教育部也在《2020年教育信息化和网络安全工作要点》中指出要加强教育系统密码应用与管理落实《教育行业密码与应用创新发展实施方案》，推进密码基础设施和支撑体系建设，有序推动教育重要业务信息系统开展密码应用安全性评估等。

财政部印发了《政务信息系统政府采购管理暂行办法》，要求采购需求应当落实国家密码管理有关法律法规、政策和标准规范的要求，同步规划、同步建设、同步运行密码保障系统并定期进行评估。公安部、住建部、交通部、水利部、农业部等国务院直属部门出台了类似的文件。

同时，各省也从政策层面对商用密码的建设从指导意见到地方规范再到资金支持，为密评的实施提供了沃土。

密评的三个重要阶段

《密码法》实施两年多来，各行各业都在加大推动密码建设落地，满足密评合规要求。在这个过程中，诸

如《商用密码应用安全性评估 FAQ（第二版）》等越来越多、更具实操性的指导性文件还会陆续发布或版本迭代，更好地指导和推动行业密码建设的落地。

总结来看，密评的主要流程主要包括以下三个阶段。

首先是设计阶段，需要对现有系统或新建系统提出商用密码改造或规划的方案。方案经由国家认证的密评机构进行审阅，若审阅通过，则将此方案在国家密码管理局进行备案。

其次是实施阶段，信息系统建设方根据方案作为指导来进行实施，对现有系统改造或对新系统建设。实施完成后，测评机构会对照方案对信息系统进行实际的测评。

第三是运行阶段。相关机构要保障信息系统的完全运行、制定应急响应。三级密评（与等保类似，密评也分为 1~4 级，级别越高，安全性越强）需要每年经过测评机构检测。

密码合规建设的四大痛点

不过，想要顺利通过密评，并非一件容易的事情。作为网络安全的基石，密码技术的建设面临着诸多难题。

第一是建设成本高的问题。在推动信息系统密码应用改造过程中，无论是设备采购的成本还是人力成本都不是一个可以忽视的数字。用户关心的是如何建设，才是密码应用合规建设投入与产出的最优性价比。譬如，部署防火墙只需接线、上电并进行配置即可上线；而在密评合规建设中，部署密码设备则需要信息系统开发商、密码厂商合作，在信息系统开发、联调、测试完全通过后才能上线。而后者的人力成本是前者的数倍。

第二是密评合规平滑过渡的问题。在预算相对紧张的情况下，怎么设计信息系统，未来才能过渡演进，以满足密评合规的要求，从而降低甚至避免为密评合规而对信息系统进行不必要的二次开发改造。因此，一套适用于客户将来能满足密评合规的演进路线就非常重要。

第三是开发者友好的问题。密码技术的应用过程，是将封装的一个个密码算法接口供上层信息系统调用，本质上属于技术开发范畴，因此密码应用的开发者友好问题就比较重要。

当前信息系统中使用最多的密码技术仍然是 RSA、AES 等国际密码算法，由于这些国际密码算法和协议在开源密码算法库中得到了广泛的支持，并且在不依赖特定密码硬件产品即可满足业务开发、调试、集成测试和上线运行，为开发者提供了友好的开发接入体验，也使得信息系统嵌入国际密码算法比商用密码算法更简单易行。

相比而言，使用商用密码算法就不得不事先购买合规的密码产品，并使用密码设备底层诸如 SDF/SKF 的开发接口或基于这些接口封装的 OpenSSL 引擎，因为开发、测试强依赖于密码硬件，提高了商用密码使用门槛，是阻碍商用密码应用在开发者普及的主要原因。

第四是密码产品自身安全性问题。传统密码产品自身安全能力仍然薄弱，安全能力有待提升。在冬奥重保的早期，奇安信对所有的信息系统、安全系统和密码系统均进行了渗透测试，暴露出了大量密码产品的安全问题。

对于密码产品而言，其承载了信息系统数据加密使用的密钥等信息，一旦密码系统遭到攻击，导致密钥不可恢复，对于系统可用性的影响是难以估量的。

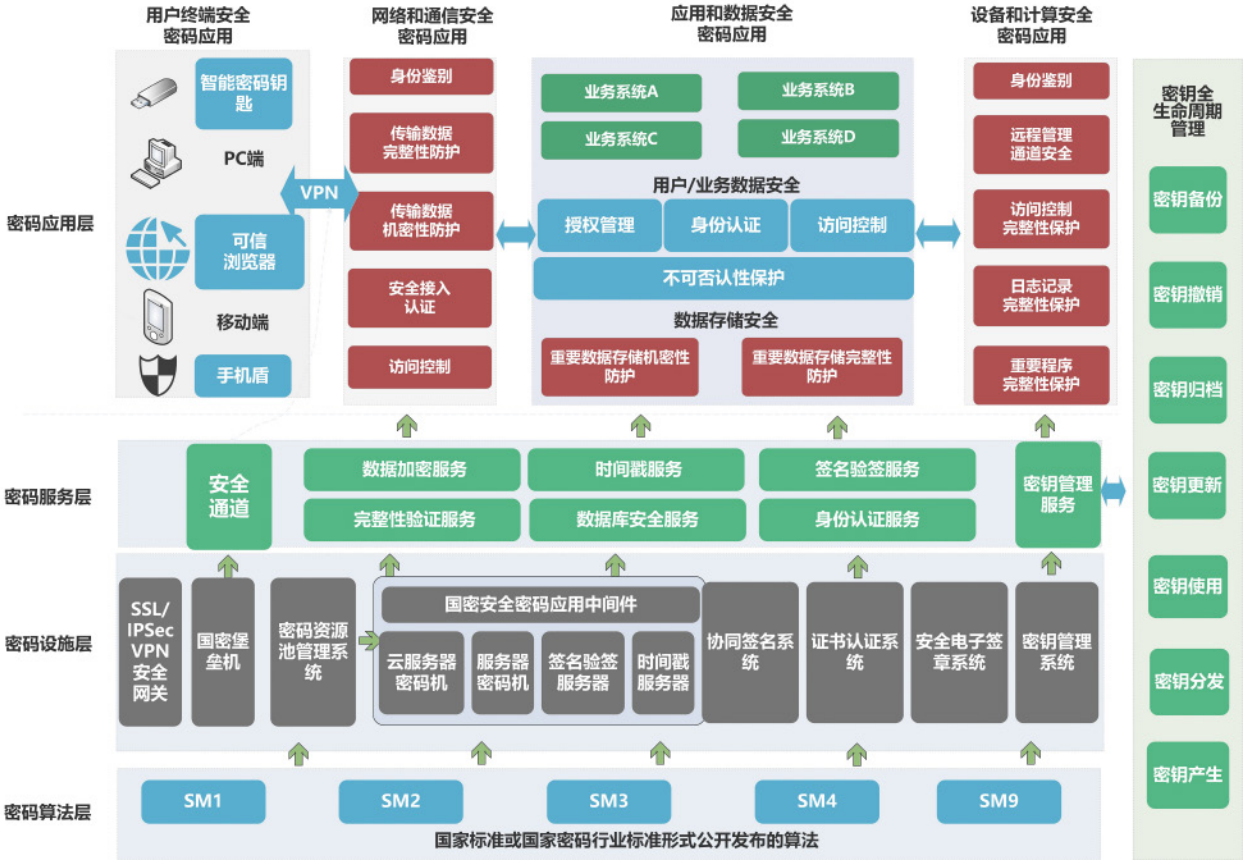
奇安信商密解决方案助力通过密评大考

针对上述几大痛点，奇安信密码安全专家给出了以下几点建议。

第一，在密码建设上除满足合规底线外，首先应考虑密码应用的“降本增效”，选择一些具有技术创新性的密码产品，在人力成本、防护效用之间找到平衡且符合自身需求的密码供应商。

第二，在预算相对紧张的情况下，筹划好信息系统未来如何满足密评合规的演进路线。这就需要咨询专业的密码厂商，在信息系统设计之初就要考虑未来能演进到密评合规的技术方案，从不合规演进到部分信息系统合规，再到全部信息系统合规。

第三，在选择密码产品时，要充分关注密码产品自



身的安全性问题。这些密码产品自身安全问题，并不在国家密码管理部门所要求的密码产品认证技术检测范畴中，也不在密码应用安全性测评机构测试范畴中，容易形成一个安全真空地带，一旦被利用和攻击，后果不堪设想。

在密评合规技术应用上，奇安信为客户提供了完整的密码应用解决方案，具备以下四点优势。

首先，商用密码产品体系完备，奇安信已经推出包括服务器密码机、密码卡、签名验证服务器、安全认证网关、安全网关等密码硬件产品，以及国密安全密码应用中间件、可信浏览器、身份认证系统、密钥管理系统、手机盾、电子签章等密码软件系统产品，满足客户不同场景下的密码建设需求。

其次安全保障体系完善，奇安信已经完成了信息系统密码应用与网络安全等级保护、零信任建设等的有效集成，打造了网络安全、数据安全、密码安全有机融合的信息安全保障体系。

第三是密码服务完整，奇安信拥有专业密码技术服务团队，团队支持政务、医疗、公安、金融、保密、物流等众多行业的密码合规建设，为客户提供售前、售中、售后全过程的商用密码应用解决方案及技术咨询。

最后是实施部署保障完全，奇安信密码产品已应用于北京冬奥会、国家及各省疫情防控平台等若干重大项目中，以帮助用户快速建立起合规、正确、有效的密码应用，满足主管部门监管需求和业务应用需求。

从 2018 年至今，奇安信持续参与相关标准编写，熟知部标前后变化和变化背后的业务要求，交付了近 200 个密码应用方案，在各部省市客户的密评及密码改造工作过程中，积累了一套从规划、设计、研发、交付到服务的商密改造最佳实践，有效助力客户改造后的业务系统符合部标，满足地方特色需求，实现高效的部署运行，轻松应对密评“大考”。

奇安信

新一代网络安全领军者

「零事故」安服团队重磅力作

900余次实战攻防演练的经验总结

从红队、蓝队、紫队视角全面解读攻防演练

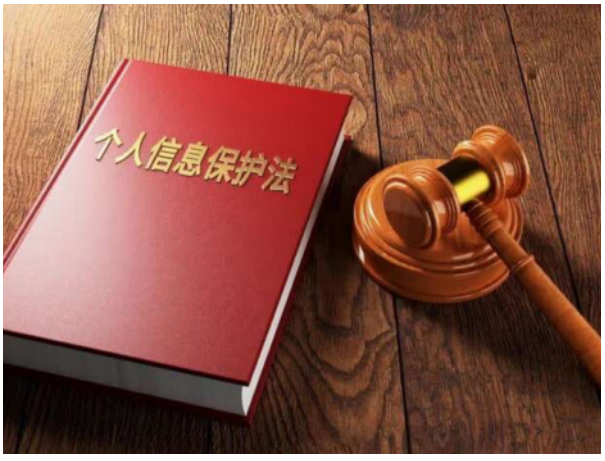
扫码购买

合规实践

《个人信息保护法》将迎实施一周年 企业隐私合规需治理先行

作者 奇安盘古 赵帅

2022 年 11 月 1 日，《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）即将迎来实施一周年。作为国内首部个人信息保护方面的专门法律，其与《民法典》《网络安全法》《数据安全法》《电子商务法》《消费者权益保护法》等法律一起，共同编织成一张消费者个人信息“保护网”。



《个人信息保护法》中明确要求：不得过度收集个人信息、大数据杀熟，并对人脸信息等敏感个人信息的处理作出规制，同时还完善了个人信息保护投诉、举报工作机制等。可以说，该法律为企业开展数据工作划定红线、明确原则、提供遵循，对企业过度收集、滥用个人信息，违规处理用户数据等顽疾，下了一剂猛药。

《个人信息保护法》实施一年以来，因隐私泄露引发的数据安全事件屡见不鲜，由此引发主管部门处罚和通报的案例更是接连不断，企业尽快推动合规落地、满足监管需求，已是当务之急。

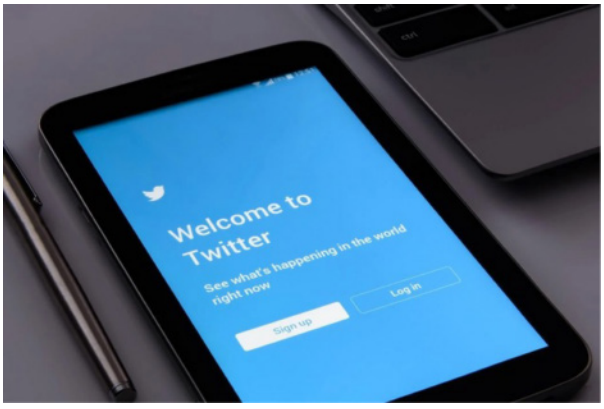
推特被罚 10 亿、某出行巨头被罚 80 亿 隐私保护亟待重视

2021 年 5 月，据多家媒体报道，美国司法部与美国联邦交易委员会（FTC）宣布，已就 Twitter 侵犯用户隐私一案与推特（Twitter）公司完成和解，将要求推特支付 1.5 亿美元（约合人民币 10.1 亿元）的罚款。

2022 年 7 月 21 日，据“网信中国”消息，国家互联网信息办公室依据《网络安全法》《数据安全法》《个人信息保护法》《行政处罚法》等法律法规，对国内某出行巨头进行了 80.26 亿元人民币的顶格罚款。

除了巨额罚款，由于忽视隐私保护，有很多 APP 被工业和信息化部通报和下架，给企业经营和声誉造成严重影响。根据工业和信息化部的数据，截至 2022 年 6 月，我国连续组织开展 APP 侵害用户权益专项整治，累计通报、下架违法违规 APP 近 3000 款。

无论是推特因数据滥用、泄露被罚，还是国内出行巨头被巨额罚款事件，都体现了国内外对隐私保护的重

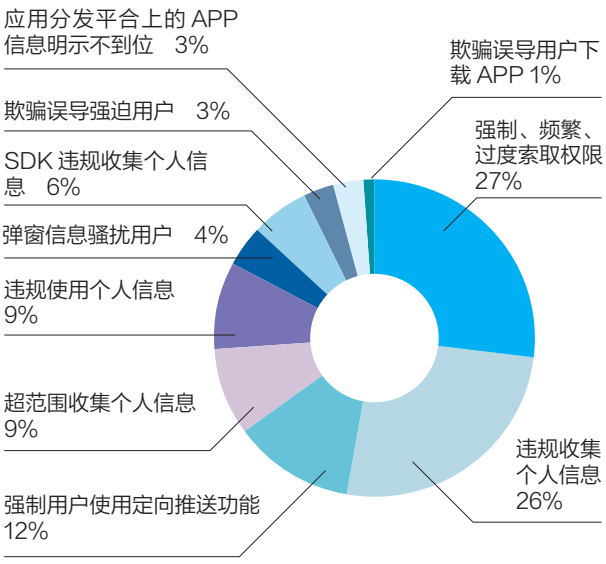


视，以及相关法律和条令的惩罚执行力度。尤其是国内，在《数据安全法》《个人信息保护法》等法律推动之下，隐私合规已经成为包括企业经营的必选项。

例如，在《个人信息保护法》中明确提到，如果由于个人信息的任何泄露、篡改或丢失而导致数据泄露，数据处理者必须及时通知主管部门和受影响的数据主体，而不仅仅是如果它“可能对自然人的权利和自由造成高风险”。同时，第五十八条对于“重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者”，要求“成立主要由外部成员组成的独立机构对个人信息保护情况进行监督”并“定期发布个人信息保护社会责任报告，接受社会监督”。

《个人信息保护法》中的相关规定，充分折射了当前企业在个人信息保护方面存在的两大合规软肋：其一是重业务而轻合规，过度索权频繁发生；其二是缺乏专业的第三方合规检测机构。

以某出行巨头被罚款为例，奇安盘古分析发现，其主要违法行为涉及多个 APP，涵盖过度收集个人信息、强制收集敏感个人信息、APP 频繁索权、未尽个人信息处理告知义务、未尽网络安全数据安全保护义务等多种情形。此外，企业自身合规意识不强，且缺乏专业的第三方合规检测机构，管理机制和技术手段均存在短板。



综合上述的大额处罚案例中，其违法收集、过度收集、未明示目的等违法处理个人信息行为，与《个人信息保护法》等所要求的合法、必要、正当、诚信原则相违背，未按照相关法律法规规定和监管部门要求，履行网络安全、数据安全、个人信息保护义务，给国家网络安全、数据安全带来严重的风险隐患。违规处理个人数据的行为可能覆盖数据收集、使用、共享等多个环节，在手机 APP、IoT 设备、网站、小程序、SDK 等数据收集端，以及对应的后台服务器上，都可能存在合规风险和安全风险。

隐私合规应治理先行 通过专业机构有效降低风险

在过去的各行业发展过程中，先发展、后治理的现象普遍存在，所以出现了违规收集、数据滥用、数据泄漏等严重侵害用户权益的现象。随着近几年监管单位的联合治理推进，《个人信息保护法》《数据安全法》等法律法规的实施，许多违法违规乱象已明显好转。奇安盘古认为，企业的发展模式也需要随着监管政策的变化进行转变，由原来的先发展后治理，转变为治理先行。从落地实施层面来看，企业在隐私合规落地过程中可能面临如下挑战。

一是没有相关经验，不知道怎么做，整体的合规意识及合规制度缺失；

二是没有相关人员，不知道谁该去做，缺少有专业资质及相关能力的合规人员；

三是没有相关技术，不知道问题出在哪，被通报后病急乱投医，到处找问题，最后依然被处罚；

四是没有评价标准，不知道做的好不好，对监管政策及相关标准不理解，即使做了大量工作，依然漏洞百出；

五是合规成本过高，需要多个部门通力协作，长期处于高压状态。

综合上述情况，企业可以通过第三方专业机构提供量身定制的合规方案，在资源有限的前提下完成合规风险有效降低。奇安盘古在过去几年的企业服务过程中，根据合规业务的特点，以及企业运营过程中的实际情况，通过产品、服务结合的方式，对客户的研发管理流程、跨部门协作方式、专业人员资质及能力等方面提供优化策略，帮助企业寻找适合自身发展方式的合规方案。

前车之鉴敲响警钟 隐私合规应遵循五项原则

国内出行巨头数据泄露这一事件为国内企业敲响了警钟，关于“企业如何做好隐私合规工作，保障个人信息安全”这一重要命题，奇安盘古从隐私保护角度给出了几方面专业建议。

首先，企业要满足政府监管要求。目前，网信办、公安部、工信部、市场监管总局及地方监管、行业监管等都在履行个人信息保护相关监管职责，且相关法规要求、标准等内容紧密出台，企业应根据自身业务属性，识别应满足哪些监管要求，根据相关法规要求内容确定合规基线。

第二，企业应自查自测发现问题并及时整改。根据相关法规要求，个人信息保护合规内容通常会覆盖企业的内部制度流程合规、个人信息收集工具如 APP 等的技术要求合规、隐私政策协议内容合规、数据收集后的安全防护要求、数据对外共享合规等诸多方面内容，企业应定期进行自查，通过调查问卷、访谈、技术检测等方式发现合规风险问题，并及时制定合适的整改方案，协同各个部门进行整改。

此外，还应建立个人信息安全事件处置机制，面对可能突发的个人信息安全事件，提前准备合适的处置预案，根据预案，在事前定期进行培训和应急演练，在事中记录事件内容，评估事件可能造成的影响，采取必要措施控制事态，消除隐患；及时与监督、管理部门保持沟通，通报或报告个人信息保护和事件处置等情况，在事后对个人信息安全事件进行复盘总结，发现问题原因，提升个人信息保护水平，并根据事件影响对相关人员进行追责。

第三，企业要不断优化合规能力。合规建设是一个持续的过程，合规能力的建设也是一个逐步完善的过程，

并不是买了多少产品、投入多少人员就能一下子解决全部合规问题。企业通过定期自查发现合规风险后，应分析问题原因，发现合规短板，对自身的合规制度流程进行完善，对人员技术能力进行提升。通过持续有效的个人信息安全影响评估活动，可以发现个人信息保护工作中的风险点，通过对这些风险的跟踪及修复，能够不断提升企业或组织的个人信息保护建设水平。

第四，企业应在遵守国家数据保护、隐私保护法律的前提下促进业务发展。个人信息保护合规建设工作不仅仅是编制隐私政策文件，简单修改公司产品、增加提醒和通知等内容，企业或组织还要将个人信息保护真正融入到日常的业务和产品中，才能让个人信息保护不再流于表面。随着监管执法力度的加强，企业或组织在管理体系建设方面的完备性和有效性验证，需要管理和技术手段并行，并且嵌入到企业或组织系统及业务开展过程中，从根本上建立健全个人信息保护管理体系，为数据价值的发挥助力。

最后，建议企业使用专业、可信赖的隐私安全产品。例如，由奇安盘古隐私安全团队推出的奇安信隐私卫士，其能够立足于解决企业的个人信息保护合规风险问题，针对安卓 APP、iOS APP、小程序、IoT 设备进行隐私合规检测与分析，帮助企业对相关业务应用进行全方位的隐私安全合规检测，提前发现合规隐患，避免由此带来的数据泄漏、资产损失、监管处罚等风险，最终帮助政府、研究机构、企业等更好地履行其在个人信息保护方面的责任和义务。

结束语：

《个人信息保护法》实施，是《网络安全法》《数据安全法》之后，我国信息安全保护在法制道路上的又一个里程碑，它将微观个人的信息安全，与宏观社会和行业的数据安全、网络安全等紧密联系到一起，共同成为国家安全战略的重要组成部分。奇安盘古基于多年隐私保护的经验，以隐私卫士产品为基础，围绕企业内部的合规要求及合规资源，可量身定制隐私安全合规解决方案，帮助企业降本增效，提高合规能力，降低合规风险。

乌军抱怨星链卫星网频繁中断，重要时刻如何守住安全底线？

作者 研究员 张少波

在乌克兰反攻俄军重要时刻，星链卫星网频繁中断，一度登上媒体热搜。近日，俄罗斯电视台网站援引英国《金融时报》报道称，据乌克兰官员和士兵证实，乌军在战场前线使用的星链（Starlink）通信设备出现故障，阻碍了乌军从俄军手中收回领土的步伐。

这位乌克兰政府高级官员表示，最近几周，部分中断事件已经引发“灾难性”的通信瘫痪。他特别提到，上报通信问题的大多是冲破前线、争夺俄罗斯控制领土的士兵，其中不少还身在交火区域之内。

据悉，星链终端由埃隆·马斯克的美国太空探索技术公司（SpaceX）制造，截止目前，马斯克和SpaceX公司均未回应置评请求。马斯克在推特上回应称“关于战场上发生的一切，都属于机密”。有媒体分析推测，可能是俄罗斯神秘的电子战系统 Tirada -2S 专门干扰通信卫星，切断了为乌军提供卫星互联网服务的星链卫星。

图：俄乌冲突中的士兵（源自网络）

重要时刻 网络瘫痪或左右战局

当今世界，网络空间已成为继陆、海、空、天之后的第五大主权领域空间，也是国际战略在军事领域的演进，网络空间安全本质上就是国家主权安全。在两国交

图：网络空间五大攻击威胁

战中，谁率先瘫痪了对方的网络通信，谁将牢牢掌控战场的主动权。

1991 年海湾战争中，美国最早将网络攻击引入军事战争，中央情报局通过特工对伊拉克从法国购买的防空系统注入病毒芯片，最终导致伊拉克指挥中心失灵，最后伊军只有挨打的份。

而到了 2007 年，为了将叙利亚核计划扼杀于萌芽之中，美军“舒特”攻击系统通过远程无线电入侵，瘫痪雷达、无线电通信系统，使叙防空系统处于失效状态。业内人士认为，作为针对组网武器平台及网络化信息系统的新型网电攻击系统，“舒特”代表着军事技术和作战方式的发展趋势，势必将带来全新战争景观。

在 2022 年的俄乌冲突中，SpaceX 的星链卫星通信系统已成为乌克兰与俄罗斯作战的“生命线”。比如在军事作战方面，乌克兰部队在手机网络中断的情况下依靠星链保持上下级指挥联络；在宣传外交方面，乌克兰总统泽连斯基通过星链与全球政界人士举行 Zoom 电话会议，并发布社交媒体内容更新，从而与俄罗斯开展宣传对抗；在日常联络方面，乌克兰军人和平民通过星链加密卫星通信与外界保持联系，了解战场局势动态，并互通安危情况。

正因为对星链卫星网络的依赖度如此之高，在乌克兰反攻重要时刻的网络频繁中断，才引起了业内如此大的关注。

重要时刻、重要业务“不中断”，是网络安全的底线

战场上，通信网络瞬息之间的中断，极可能导致上下级指挥失联，轻则殆误战机，重则满盘皆输。而在政企机构的运转中，因网络故障导致的业务中断，同样会造成巨大的损失。

2021 年 5 月，美国最大的石油管道公司之一 Colonial Pipeline 因遭受勒索软件攻击而被迫关闭。迫使美国 17 个州和华盛顿特区采取紧急措施，引发业界震惊。美联社报道称，这是美国关键基础设施迄今遭遇的最严重的网络攻击。

奇安信集团董事长齐向东认为，这次事件给我们敲响了警钟，这是全球首次因为网络空间导致物理空间危机、并不得不启动紧急措施的事件，再次凸显了关键基础设施的脆弱性。

重大活动、重要时刻，也往往是网络攻击肆虐的舞台。5 月 9 日，在俄罗斯举行胜利日阅兵的重要时刻，该国智能电视显示的画面遭到篡改，展示了许多反战标语信息；俄罗斯主要电视频道、最大搜索网站 Yandex、最大视频网站 RuTube，均受到网络攻击的影响，使

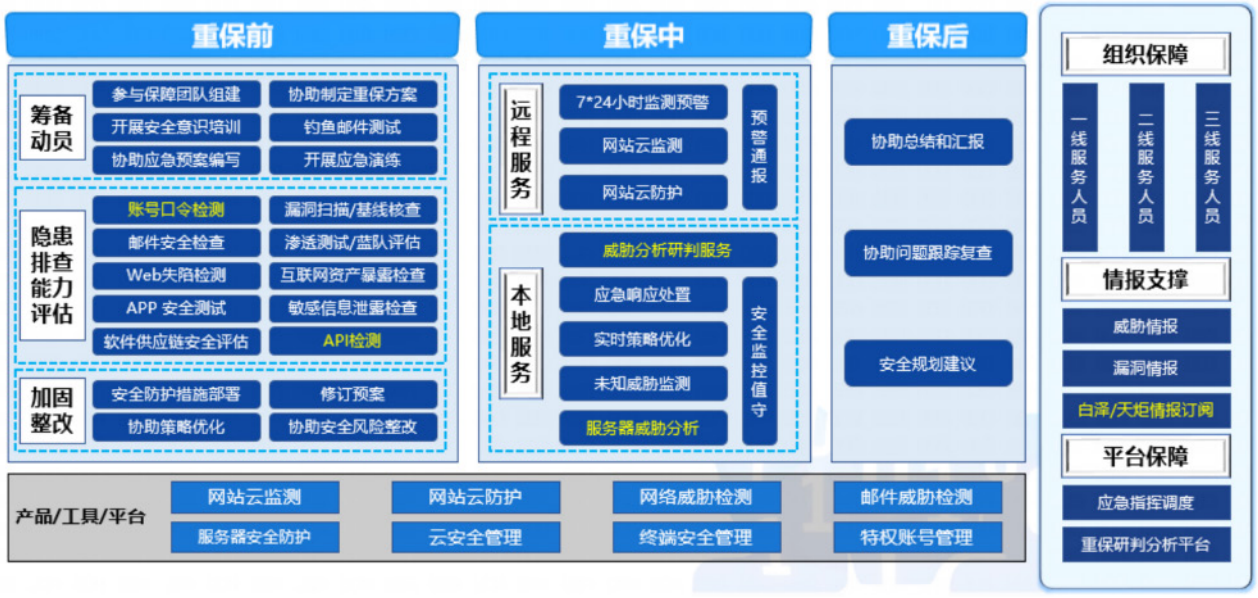
得胜利日阅兵无法顺利直播。

作为中国电子政务平台的第一堡垒，云上贵州负责人曾透露了一组数据，在我国重大节假日和庆典前后，海外网络攻击量常呈数十倍增长，网络安全的压力可想而知。

在 7 月 13 日的 2022 年北京网络安全大会（BCS2022）上，齐向东曾表示，网络安全“零事故”具体有三条标准，第一个就是“业务不中断”，在数字时代，业务变得越来越开放互联，一旦中断，就可能是重大网络安全事故。轻则营业收入、口碑受损；重则触犯法律，直接威胁社会生产生活和国家安全。

重要时刻亟需可靠的重保服务

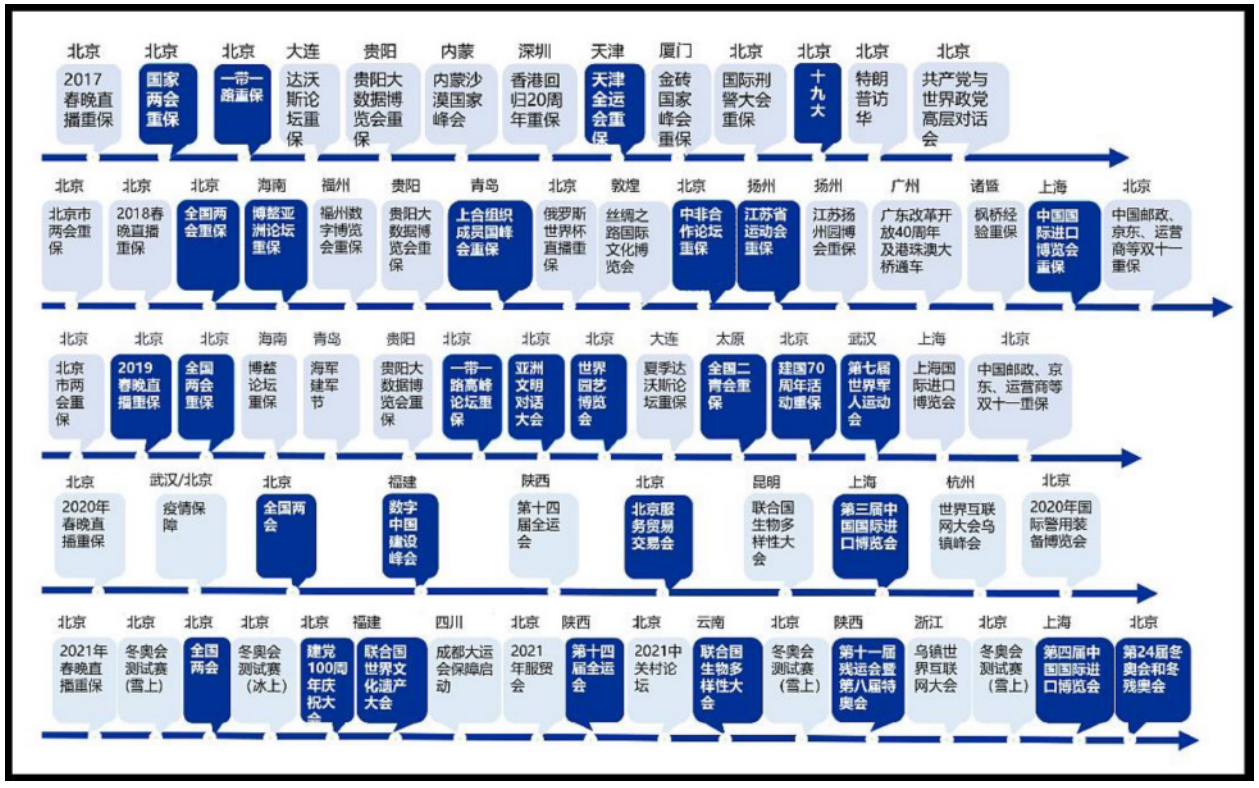
众多事实证明，国际会议、国家会议、大型活动、节日庆典等重要时期，往往也是国内外各类攻击组织最为活跃的时期，大量关键信息基础设施、政企机构内外系统都会成为网络攻击的重要目标。一旦发生恶意破坏、恶意篡改、数据泄露、系统停服等重大网络安全事故，不仅会带来严重的经济损失，还会产生重大的社会影响。



为此， 奇安信集团为政企机构提供重要时期的全方位网络安全保障支撑，即重保方案。该方案以保障网站和系统、网络安全为核心，以防攻击、防入侵、防篡改、防窃密为重点，从系统安全、主机系统安全、数据安全及应用安全等层面，提供“前期清隐患”“中期控风险”“后期深复盘”三个阶段完整的安全保障服务。确保客户在重保时期，有效防范网络安全重大风险，遏制网络安全重大事故，实现不出事故、不被通报。

强大的安全服务能力，是奇安信重保方案的突出优势。在 2022 年北京冬奥会和冬残奥会中，奇安信作为奥运史上首家第三方网络安全服务商，交上了北京冬奥会、冬残奥会网络安全保障“零事故”的答卷。“零事故”充分证明了奇安信的技术实力和服务能力，经过奥运会级别的重大活动考验，为行业树立了新标杆。

奇安信还具备业内领先的情报和威胁检测能力，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，连续三年夺得中国安全分析和情报领域第一位。 截至 2022 年 6 月，奇安信已累计首发 15 个国内外 APT 组织，监测到的针对国内发动 APT 攻击的黑客组织达到 49 个。安



NGSOC+MSS 王炸组合显身手
某母婴品牌 HW 逆袭全市前五

作者 安全运营 BG

出于对客户信息保密，本次案例的客户名称用 B 品牌来表述，其母公司用 X 集团来表述。

提到 B 品牌，许多人可能并不熟悉，但对于关注母婴健康的父母来说，B 品牌早已名声在外。

B 品牌于 2016 年申请成功，是杭州某实业有限公司旗下的母婴品牌，隶属于 X 控股集团有限公司（以下简称 X 集团）。2022 年 3 月 28 日是 B 品牌首秀，只能说 B 品牌确实低调，甚至有点“怪”。它不仅很少做大型广告营销事件，甚至连设计理念，都是听着很反直觉的“存在即不合理”。

然而正是这样一家公司，在成立之初就制定了一站式全品类战略，并在行业率先成功实现全品类布局。据统计，B 品牌的产品目前已覆盖了母婴行业的 33 个二级类目，近 600 个三级类目，而且绝大多数类目 B 品牌都有着不俗的表现。据天猫渠道数据显示，2021 年该品牌在背带、湿巾、牙膏牙刷、水杯餐具、睡袋床品等多个二级类目中占据了前三位置，且 TOP 类目数量同比增长高达 86%。目前 B 品牌在 30 多个国家服务超 4500 万家庭，天猫官方旗舰店粉丝数量超过 1600 万，稳居行业榜首。

这样一家做到行业领先的公司，却因为安全运营做的不够完善而苦恼，还因为每年的 HW 成绩排在全市（杭州市）百名开外而惶恐，亟需寻找网络安全领域最专业的企业帮其构建安全运营体系。

“我们从产品角度选择合作伙伴都是挑选全球最专业的机构合作，比如，美国的莱卡（LYCRA）是纤维创新领域的行业领导者，新加坡的赛得利（EcoCosy）是全球最大的纤维素纤维生产商，德国的汉高（HenKel）具有 140 年的历史，我们使用汉高 ON“合护”创新技术对纸尿裤进行技术改进，还有德国的德之馨（Symrise）、美国的陶氏化学（DOW）等。我们的企业理念是，凡是供应商都找最专业的，因此在选择安全厂商的时候，也经历过多家安全厂商的选择和考察，最终选择了奇安信。”作为 B 品牌的母公司，X 集团安全负责人说。

HW 成绩从百名开外逆袭全市前五

HW 分为国家级、省级、市级，市级 HW 由本市公安组织针对市级重点单位进行，X 集团具有员工 4000 多人，目前在母婴领域已属知名企业，多次被杭州市公安部门选为参与市级 HW 的重点企业。然而，以往的 HW 成绩却不理想。

“历次杭州市级 HW，被选中的政企机构数百家，在最后成绩排名时，X 集团以往最好的成绩还在百名开外，这样的实战检验让公司高层很惶恐。公司越做越大，却有个薄弱的后门，万一哪天突然中个勒索病毒，面临的损失无法预测。于是公司开始重视并加强网络安全建设，保障 X 集团在全球的业务运营，也保护我们在客户面前的良好声誉。”

2022 年 HW 刚过去几个月，这次的 X 集团终于扬眉吐气了一把，成绩排名全市第五。这不仅仅是安全防护能力的证明，也是对过去两年的安全建设成果的检验。

2022 年 5 月 19 日，X 集团接到辖区公安通知，被杭州市 HW 选中，因为有了这两年奇安信的加持，这次 X 集团的信心比以往强多了。除了以往已经部署的天擎、ICG、BASS 等产品，在 2021 年 11 月还部署了奇安信态势感知与安全运营平台（NGSOC）、统一服务器安全管理系统（椒图），并且同时加强了安全运营，接入到奇安信安全运营中心，使用 MSS 服务。

然而在 HW 期间，为了将安全防护建设的更加牢固，多一重保障，X 集团安全运营团队还特意选在这个时期

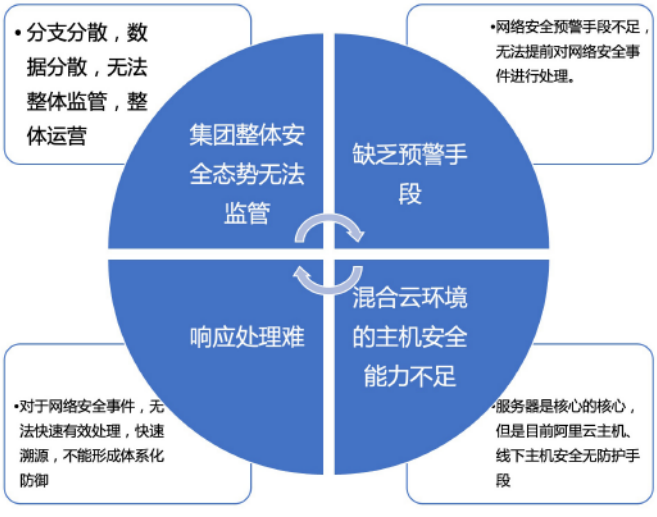
序号	防御单位团队	积分	总提交数
1	[redacted]局	11528	6
2	[redacted]员会	11436	5
3	[redacted]限公司	11284	4
4	[redacted]中心	11228	3
5	杭州[redacted]实业有限公司	11150	3

对其他厂商的安全产品进行测试，但测试结果很不理想。友商的被测试产品在 HW 过程中被打穿了，NGSOC 第一时间发出高危告警，运营人员利用 NGSOC 进行响应处置，并通过平台溯源功能还原了整个事件过程，编写了事件分析报告，在这次 HW 中获得大幅加分。

这次的 HW 成绩，不仅让 X 集团高层及安全运营团队加强了信心，也对奇安信的专业产品和专业服务更加信赖，同时友商也在这次 HW 中以被悲惨吊打的结果被迫出局。

专业的安全建设是取得好成绩的前提

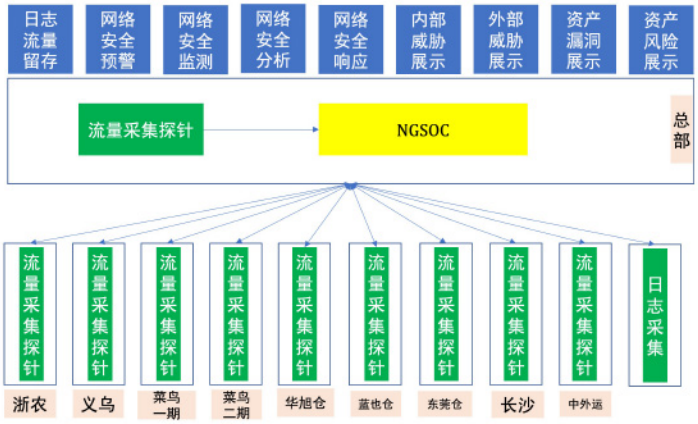
在与奇安信合作之前，X 集团面临的网络安全问题



与大多数企业类似，企业发展规模越来越大，分支机构越来越多，信息系统越来越复杂，数据越来越重要，客户对个人隐私越来越敏感。国家对网络安全越来越重视，监管部门对网络安全要求越来越高，同时外部的网络安全环境也越来越复杂，勒索病毒盛行，对企业的安全带来新的挑战。

然而 X 集团整体安全态势无法监管，缺乏预警手段，即便有预警手段，响应处理也是难题，且混合云环境的主机安全能力不足。

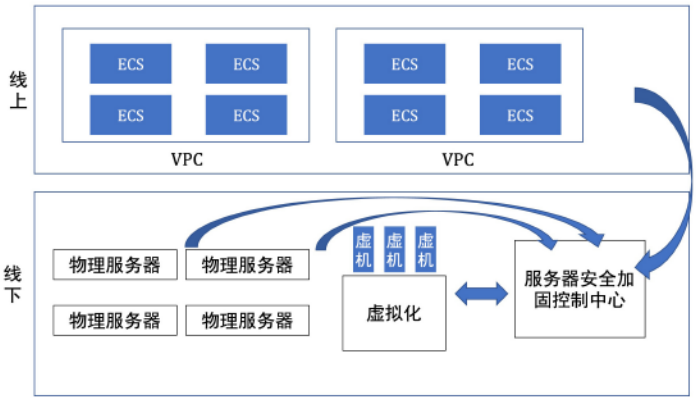
· 部署 NGSOC 统揽安全大局



2021 年 11 月，X 集团在总部部署 NGSOC，通过对流量和日志的采集、发现、分析、通报相关的网络受攻击、威胁和风险情况，提升集团的网络安全监测预警、信息通报、应急响应和重要时期安全保障的能力。在全国分支部署流量采集探针，实现对指定范围内的网络与信息安全的集中、全面、深入监测，及时发现安全隐患及威胁并分析处理。最后再通过 NGSOC 平台对集团的网络安全进行统一管理、运维、处置管理、漏洞管理等。

· 部署椒图 云上 / 云下服务器统一管理

针对混合云环境下的主机安全问题，采取的方案是在总部统一服务器安全管理系统（椒图），对



阿里云和线下服务器进行统一管理，配置下发，日志采集。在所有服务器上安装部署 Agent，实现网络及系统层攻击拦截，攻击方式捕获、漏洞发现、漏洞修复、补丁管理、系统加固、访问控制、应用隔离、威胁感知、系统资源监控、应用性能监控等。

· 接入 MSS 实现 7×24H 持续安全运营

安全攻击 24 小时都有可能发生，有了安全工具，却无法做到 24 小时持续运营；有了安全攻击，缺无法及时做到专业响应，这都严重影响安全运营效果。为了彻底解决持续运营的问题，X 集团 2021 年在部署 NGSOC 和椒图的同时，还将安全运营交给了奇安信 MSS 团队，实现本地 + 远程双运营模式，基于奇安信云端威胁情报和应急响应中心的实战攻防经验，通过安全运营指挥中心提供远程 7×24H 的跨平台监控，全面防护安全攻击。

这也是自 2021 年 9 月奇安信推出 NGSOC+MSS 王炸组合以来，第一位接入使用的客户。

奇安信 MSS 团队服务分为启动阶段、服务筹备阶段、持续运营阶段，在各个阶段分别提供不同的服务内容并交付不同的服务成果。通过持续运营，形成事件报告、事件深度分析报告、运营周报、运营月报、漏洞预警报告、漏洞修复指导等。

通过近 1 年的持续运营，发现、修复、解决了不少安全问题，不断筑牢安全防护基石，这也是今年 HW 取得好成绩的根本原因。

从告警类型数量来看：

自 2021 年 11 月开始监测，首月告警类型数量 321，次月下降 27%，至 234。

到 2022 年 8 月，告警类型数量下降至 32。

自接入奇安信 MSS 远程运营以来，MSS 团队共推送 56 条安全事件，其中一次是 webshell 通信事件，经 X 集团安全运营人员确认，不是正常业务行为，最后通过 NGSOC 查询该资产的登录日志确认事件发生时间，并找到对应项目。

专业的 MSS 运营帮助 X 集团安全运营团队检验安全薄弱环节、不断完善安全防护体系，并形成发现 – 响应 – 分析 – 处置 – 加固的闭环。截至目前，X 集团已明确将续签 MSS 服务，持续加强安全运营。

安全运营不是一蹴而就的，好的成绩也不是靠一朝一夕，安全运营需要人 + 工具 + 流程的不断完善和磨合。未来，X 集团将会加强与奇安信的合作，不断强化安全防护体系建设，完善安全运营流程制度建立，为 B 品牌成为全球母婴领头羊护航。 安

规划一步快一步

奇安信 | BEIJING 2022

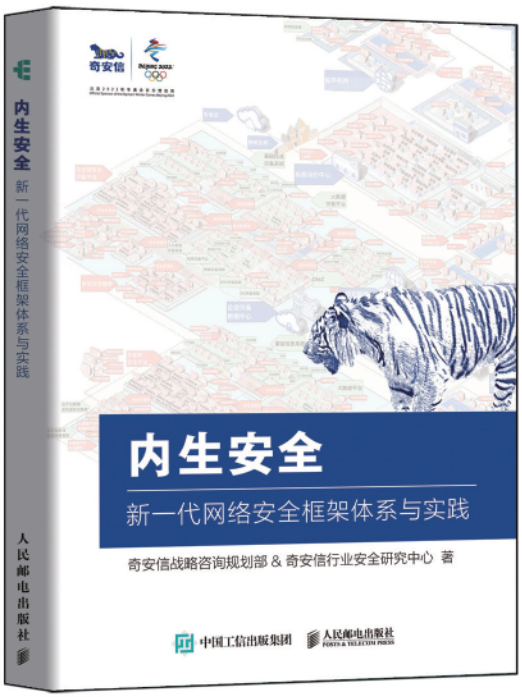
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

新书发布

内生安全权威解读

19支团队、37位专家倾力打造

政企“十四五”网络安全规划必读书籍



- 什么是内生安全
- 内生安全从何而来
- 为什么要内生安全
- 内生安全如何落地
- 新一代网络安全框架
- “十工五任”建设要点

扫描二维码
专享内购价

安全有道，合规先行

——走近奇安信战略推进中心姜晨、杨建

作者 公共部 孙丽芳

一直以来，合规作为重要驱动力，对我国网络安全事业发展起到了巨大的推动作用。作为网络安全行业的领军企业，奇安信近年来围绕合规推出了众多创新产品和服务，为政企单位提供了全方位保障。在奇安信内部，各个技术方向都高手如云，但对于合规这件事，大家总愿意听听两个人的意见——这就是战略推进中心的姜晨和杨建。

这一切，还得先从他们各自的经历说起。

殊途同归走上网安路

姜晨本科的专业是国际贸易，硕士学的是经济。这是一条看起来和网络安全没有什么交集的轨迹。“但是读研究生的时候，有一次帮导师做项目，我去调研了天融信。那是我第一次真正接触网络安全，让我对这个行业充满敬畏，觉得特别有使命担当。”

这个偶然的交集，给姜晨留下了深刻的印象，也埋下了某种伏笔。毕业两年后的 2011 年，绿盟向在一家咨询公司得到充分历练的姜晨伸出橄榄枝，邀请其加盟公司，负责对接工信、公安等监管部门。因为是自己早有好感的网安行业，姜晨欣然同意。勤奋和努力让姜晨逐渐从网安门外汉到对业务驾轻就熟。2016 年，工作业绩出色的姜晨被奇安信招致麾下，继续负责对接几大监管部门。

和姜晨毕业不久就误打误撞入行相比，杨建真正走上网络安全道路要晚一些，但称得上是水到渠成。“网络安全是国家安全特别重要的组成部分，我在北京市安全局干了十多年，所以我对这块工作并不陌生，实际工作中也经常会遇到。”2014 年，杨建离开安全系统，到某市属国企参股企业做 CEO 兼党支部书记。2020 年，杨建加盟奇安信，负责对接监管部门之外的部委和央企。“我其实一直很关注网安行业，我觉得这里肯定有我的

用武之地。”

殊途同归，姜晨和杨建先后来到奇安信战略推进中心，对接国家监管部门和政企单位。合规由监管部门主导，而政企单位又是主要合规对象，因此他们得以完整经历合规是如何驱动整个网络安全行业发展，也非常了解奇安信在其中是如何从亦步亦趋的跟随者，到积极主动的参与者，再到提前布局的先导者。

政策和事件共同驱动

“网络安全产业的高速发展，有几个重要的驱动要素。其中最重要的驱动力，就是政策驱动和事件驱动。从 2011 到 2022，就我自己亲历的这 11 年来看，我觉得有一些政策和几件大事儿真正推动了这个产业的发展。”

因为长期和主导合规的国家监管部门打交道，姜晨梳理合规驱动有自己清晰的脉络。

“中央网信办成立之前，还是九龙治水的感觉，那个时期合规最重要的抓手是等保检查。网络安全等级保护制度作为国家信息安全保障的基本制度，直接驱动了当时的网络安全建设。中央网信办成立之后，就是党管安全了。次年《网络安全法》的出台让整个行业为之振奋，我们作为安全从业者，切身感受到了国家对网络安全的高度重视，以及对我们保护国家网络安全的迫切需要。随后陆续出台的《数据安全法》《个人信息保护法》《关基条例》《漏洞管理规定》等一系列法律法规，无一例外都要求政企机构必须要合规。”姜晨说，这个时候就会带来新的市场机会。

“从具体工作视角，我看到每年合规的重点关注方向都有不同，但相同点是，这些方向都引领着网络安全产业未来的发展。”

2016 年和 2017 年，姜晨给出的合规关键词是“态势感知”和“重保”

2016 年 4 月 19 日，习近平总书记在网络安全和信息化工作座谈会上发表重要讲话，提出 “要树立正确的网络安全观，加快构建关键信息基础设施安全保障体系，全天候、全方位感知网络安全态势，增强网络安全防御能力和威慑能力。”同年，多个监管部门启动筹建态势感知平台。“当时我刚到奇安信不久，正为公司真正大数据基因所赋予的能力而兴奋，于是我毫不犹豫地找到客户，毛遂自荐：奇安信有数据驱动安全的理念，这和监管思路一脉相承；奇安信有真正的大数据体系，能够打通多源异构数据；奇安信有强大的追踪溯源能力，能够帮助客户进一步挖掘有价值的线索；奇安信有一支懂业务的团队，愿意和客户一起攻坚克难。”经过姜晨和态势感知团队同事们一年多不分日夜的努力，首个由奇安信承建的态势感知平台终于落地应用了。那个画面让姜晨记忆犹新。“当时真是特别激动，就是‘十九大’网络安全指挥部现场使用了奇安信研发的态势感知平台，很多其他监管部门和政企领导也在指挥部现场值守，大家此前都没见过态势感知平台真正应用在这个级别的实战中。当时参与值守的一个领导，现场就对这个平台非常感兴趣。十九大结束后我们业务团队迅速跟进，不到一年的时间奇安信承建的威胁共享平台和应急指挥平台也呈现在了他们的指挥大厅。”正是那一年，奠定了奇安信在几个头部监管机构态势感知平台建设主体的位置，进而形成了良好的标杆示范作用。“就在最近，我们和公安部三所评估中心联合申报的‘关键信息基础设施安全保护关键技术与应用’荣获了公安部科学技术奖一等奖，这是首个在关键信息基础设施安全领域获得的一等奖，充分说明了对奇安信关基保护技术能力的认可。”

“2017 年是奇安信的重保元年，也是打基础的一年。”作为公司与监管机构的接口人，姜晨这一年格外忙碌。2017 年在北京举办的首届“一带一路”国际合作高峰论坛，是习总书记 2013 年提出“一带一路”重大合作倡议以来中方召开的规格最高的国际会议，也是奇安信第一次进行公司级的投入，全方位支撑监管机构去做重保。“能够作为牵头人调动全公司资源，参与如此重要的保障任务，我倍感使命光荣，同时也深知责任重大。前期我们配合监管部门做了充分的工作准备，但令人始料未及的是，就在峰会前两天爆发了 512‘永恒之蓝’。我是半夜 2 点多被同事打电话叫醒的，当时一看公司蓝信群里都炸了，情况非常危机。我马上连夜上报，

紧急协调应急队伍赶赴现场处置。最终，我们经受住了考验。”面对这次突发的网络安全事件，奇安信临危不惧、快速响应、有效部署， 72 小时先后派出 3000 多人服务 1700 多家单位，树立起行业应急响应的标杆。正是通过这一次历练之后，公司决定在安服专门成立一个重保部门，常态化支撑各项重保工作任务。“这次重保经历让我至今难忘，保障任务结束以后，我组织 40 多个驻守在重保一线的兄弟们一起庆功，打一场胜仗才是最好的团建。”

2018 年留给姜晨印象最深的，是公安部的大数据智能化项目

“大数据时代，海量数据的产生为公安机关打击犯罪活动、维护社会治安提供了有利条件，可是如何有效解决数据共享、避免各警种单打独斗，成为当时重要的研究课题。”为此，公安部提出大力推进实施公安大数据战略，加强顶层设计，加快形成覆盖全警、统筹利用的数据信息资源服务体系。“公安数据体量大、种类多，当有重大案事件需要横纵向调动数据的时候，就需要进行授权，谁、可以在什么时间、什么地点、使用什么设备、因为承担了什么任务，访问了什么数据，这是一个典型的数据合规应用场景。而公安部的大数据智能化项目，就是要解决数据怎么打通，同时又合理授权的问题。当时主流的服务商都参与了这个项目的竞争。‘零信任’这个词就是首先在我们的方案里提出的。我带着公司战略咨询规划专家去做汇报的时候，客户眼前一亮，觉得这个概念非常好，我们提出的基于零信任的动态访问控制，很好地解决了主客体访问控制的的难题。”在零信任的基础上，奇安信延伸出公安大数据的一整套解决方案，最终在众多厂商中脱颖而出，夺得了第一名。“不仅如此，更有成就感的是，密切参与公安部大数据智能化项目为我们公司内部的数据治理和数据中台建设埋下了种子，监管关注方向已经成为牵引公司变革和创新的重要源泉。”

2019 年和 2020 年的合规重点，姜晨标在了 APP 安全

2019 年四部门联合发文，明确了 APP 收集个人信息范围，工信部等单位同步开展了规范整治 APP 违规收集使用个人信息专项行动，定期通报不合规的 APP。“为了提高检测效率，监管机构建设 APP 技术检测平台的需求应运而生，各大 APP 也纷纷找上门来寻求我们的技术支持。虽然是个全新的赛道，但对政策的高度敏感让我们早有布局。鉴于奇安盘古团队对各类移动应用全方位和深度的隐私合规检测能力，我主动向监管机构表态，积极发挥我们自身技术优势，帮助提供 APP 隐私检测技术支撑，高效配合和助力其技术手段建设和专项治理等工作，此后感谢信和订单纷至沓来。”

2021 年和 2022 年的合规重点，落在供应链安全和数据安全

“2021 年年初，中央网信办新成立了供应链处。这说明国家对供应链安全已经高度关注，同年公安部也启动组织实施了供应链安全专项。2021 年年底爆发的 Apache Log4j 漏洞，再次提醒我们盲目信任第三方软件的时代已经结束。供应链安全是一个非常重要的合规方向，早在 2021 年年初我们就开始了提前布局，基于奇安信天问平台、代码卫士和开源卫士的检测能力，我们面向监管机构提出了一套供应链安全治理方法论，并且制定了一系列切实可行的工作计划，希望可以通过有效的行业调研，形成具有价值的建议，从而加速驱动政策出台。”

“数据安全是今年最热的词，为了支撑国家数据安全产业发展，我们和公司数据安全专班密切配合，专门设立了数据安全专项，一揽子开展数据安全相关工作。今年我们的核心工作主要围绕三个方面展开。一是积极开展联合研究：今年年初奇安信联合信通院共同发布了《 2022 年数据安全风险分析及应对策略研究报告 》，报告从理论与实践层面指出了当前存在的问题并有针对性地提出了五大关键举措；二是不断提升自身供给侧输出能力：工欲善其事，必先利其器，奇安信提前投入研发，早在今年 5 月数据出境安全评估办法正式出台之前就对外发布了数据跨境卫士，支持提供一整套数据跨境合规流程的技术手段和方法。此外奇安信旗下多款数据安全产品，全部通过了信通院开展的七大品类的测评认

证，成为首家获得全套数据安全产品测评资质证书的网络安全企业。奇安信还积极参与了工信部工业企业数据安全管理试点工作，支持供给侧构建工业领域数据管理新模式；三是积极带动产业发展、支撑一流数据安全人才培养：奇安信今年牵头成立了 CCF 计算机专委会数据安全工作组，以及电信和互联网行业数据安全人才强基计划产业促进工作组，我们希望依托工作组的多方连接，盘活‘多类型数据安全人才、教育、行业用人单位、安全产业公司、政府指导机构’等多方生态，从需求侧与供给侧扩大市场与人才规模，近期我们正在积极开展数据安全人才需求调研和数据安全人才培训基地挂牌工作。”

正如姜晨亲身感受的，奇安信在安全合规中的角色非常立体，并不是被动的跟随，而往往能做到深度参与，甚至引领。“这与我们多年来和监管机构保持密切沟通有着密不可分的关系。通常情况下，在政策法规出台前，我们会积极建言献策，掌握最新动态；政策法规出台后，我们会第一时间进行深度解读，帮助大家做好消化吸收；监管机构对一些重要事件的处置我们也会参与策略制定，更重要的是还会给予技术支撑，这往往是监管机构最需要的。”

专业的人干专业的事

正是这种深度参与，让奇安信得以提前布局，围绕合规保障推出了众多创新产品和服务，主要包括等保合规、数据安全合规、密码合规、隐私合规等类别，能为企业提供全方位保障。此外，奇安信还发挥自身的人才和技术优势，协助相关部委进行网络安全工作培训，切实提升重点人群网安合规的意识、知识。这正是杨建去年以来在忙的事儿。

2021 年国资委下发通知，根据中央网信办关于网络安全万人培训计划的总体部署，利用 3 年时间，分批次对中央企业及其所属企业从事网络安全相关工作战略管理人员、技术管理人员和实战人员开展培训。这场培训的规格之高、规模之大，不言而喻。

“我们主动向国资委请缨，主要表达了三点：奇安信有这样的实力；奇安信有相应的课程；奇安信有全国范围内的虎符培训，还有内部的砺剑培训，更有和高校的产教融合成功范例，搞培训非常专业。”经过杨建和同事们的努力，最终，奇安信承担起了这项光荣而艰巨的任务，负责整体培训内容设计，包含课程设置、讲师安排及服务保障等工作。

“我们围绕习近平总书记关于网络强国的重要思想、国家网络 战略和治理、网络安全产业和技术变革、网络安全攻防演练 实战交流等，采取专班授课、主题报告、课件讲授、案例分析、攻防演练、互动交流等方式开展培训。截止目前已经开了 9 期班，培训了中石化、中海油等 8 家央企。学员都是各集团主管信息化、数字化或网络安全的负责人。”

专业的人干专业的事收到了良好的效果。参训企业对培训课程设计、讲师授课、服务保障高度认可。培训期间共发放满意度调查问卷 670 份，回收 615 份，满意度 100%。2021 年 9 月 17 日，中央网信办庄荣文主任赴培训现场专题听取中央企业专项培训工作情况，对培训工作给予充分肯定，同时对奇安信承担的中央企业专项培训工作给予了充分肯定。

“成功组织央企专项培训是我们自身实力的有力证明，也是提升公司品牌、扩大公司影响力的重要抓手。行稳才能致远，合规一直是各方关注的重点。我们的培训课程里专门就有网络安全法律法规的解读。”

日前，国务院国资委发布了《中央企业合规管理办法》。这是国资委成立以来第一个针对合规管理发布的部门规章落实办法。杨建和团队立刻对《办法》进行了深度解读。

“下一步，我们将根据前期培训成果和新出台的政策，针对性提高和丰富培训内容，进一步做好中央企业专项培训工作。同时，我们也将联合全国各省市地方国资委开展相应的网络安全专项培训工作，由奇安信组织承担相关工作，将中央企业专项培训成果和经验复制到地方国资系统，全面提升奇安信在地方国企的品牌影响力，全面支持国企网络安全工作。”

杨建在合规层面的工作不仅仅局限于此。中国通信学会数据安全委员会即将依托奇安信来建立，杨建的工作就是负责委员会的成立，以及后续秘书组的工作。目前依托数据委员会已经在推进北京市律师行业 3000 家律所数据安全团体标准建立工作，这将是对律师行业数据合规的一次全面调研、梳理和体系建立，有助于奇安信数据安全产品服务向中大型律师事务所提供全方位服务。

姜晨和杨建所在的战略推进中心是连结公司各业务线和各监管机构、部委、央企的关键一环。“这就对我们提出了很高的工作要求，工作节奏也非常快。”姜晨多年来一直留着利落的短发。“开始是觉得方便，后来就成了习惯。”杨建则多年保持着良好的运动习惯。“这算是我提高工作效率的方法”。他们两位都同时提到战推中心这个平台给予了他们无限的成长空间，在奇安信这个大平台上，在战推这个大家庭里，满怀激情，当则奋斗，拥抱变化，用自己的理想信念为奇安信早日实现十四五规划目标奋斗。

随着我国网络空间法制体系建设的完善，网络安全的合规需求将持续井喷，成为支撑产业高速发展的核心引擎之一。可以预见未来，姜晨和杨建相关的工作会越来越多。但和所有奇安信人一样，他们忙碌着，但也充实着，怀抱着“让网络更安全，让世界更美好”的初心。 安

奇安信 | BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

奇安信威胁情报中心

中国威胁情报行业领军者

奇安信威胁情报中心是奇安信集团旗下专注于威胁情报收集、分析、生产的专业部门，以业界领先的安全大数据资源为基础，基于奇安信长期积累的威胁检测和大数据技术，依托亚太地区顶级的安全分析师团队，通过创新性的运营分析流程，开发威胁情报相关的产品和服务，输出威胁安全管理与防护所需的情报数据，协助客户发现、分析、处置高级威胁活动事件。

威胁情报中心

威胁研判分析平台ALPHA： 一站式云端SaaS服务的威胁分析工具平台。是安全分析师为同行打造的利器，针对IOC查询、线索关联、事件溯源、样本行为检测和同源分析等威胁分析场景提供全面的解决方案。

高对抗云沙箱分析平台： 提供多种动静态检测、分析技术，展现文件各方面特征，帮助分析师快速判别、并掌握恶意软件的详情。

威胁分析武器库： 服务于安服、安运、安全分析师及各类企业用户。支持IOC自动化数据流检测、失陷情报、恶意IP批量查询；支持邮件批量自动化检测；支持WEB应急日志、主机应急日志分析。

威胁情报系统QAX TIP： 威胁情报平台是情报收集、维护、使用的综合性平台。可帮助企业在安全运营中，利用威胁情报快速检测、响应、分析和预防各类网络攻击威胁，并分析产生行业威胁情报。

威胁雷达： 利用大数据和威胁情报监测技术，整合了奇安信的高、中位威胁情报能力，提供指定区域内网络威胁高位监控、案件拓线分析、样本深度分析等多种能力。

样本同源分析系统： 奇安信威胁情报中心红雨滴团队基于样本基因深度解析，使用机器学习算法用于APT数字武器追踪的可视化分析系统。

高级威胁分析服务： 为网络安全主管单位、政府机构、行业客户及高校科研机构提供情报线索拓线和威胁分析服务，输出深度分析报告供其决策参考。

奇安信威胁情报中心：
ALPHA网址：https://ti.qianxin.com
雷达网址：https://r.ti.qianxin.com
扫描关注我们的微信公众号
邮箱：ti_support@qianxin.com

保障业务不中断！奇安信专项整治挖矿、勒索、DDoS“全员恶人”

作者 公关部 王梦琪

在武侠世界中，金庸曾在《天龙八部》中塑造出有名的“四大恶人”，令江湖人闻风丧胆，他们分别是恶贯满盈段延庆，无恶不作叶二娘，凶神恶煞岳老三，穷凶极恶云中鹤，个个行事穷凶极恶。而在网络安全的世界中，DDoS 攻击、勒索软件和挖矿木马，这三种常见且高发的网络攻击方式，同样是笼罩在各行各业、政企组织上方的一片乌云，往往为业务正常运行带来“灭顶之灾”，组成了安全圈的“三大恶人”。

“三大恶人”频繁作乱 重要时期业务中断成核心痛点

中断业务的“三大恶人”之 DDoS 攻击

2022 年 2 月，俄乌冲突伊始，伴随着俄军在乌克兰首都和重要城市带来的轰炸声，前所未有的 DDoS 攻击同时进行。在两国爆发冲突的重要时期，乌克兰国防部、武装部队、外交部和内政部的网站因遭受 DDoS 攻，击对外界访问请求不能响应或加载缓慢。另一方面，俄罗斯电视台、克里姆林宫、俄罗斯国防部、外交部等多个政府部门，同样因 DDoS 攻击而无法访问相关业务。

利用大量肉鸡发起访问，导致系统业务无法正常操作的 DDoS 攻击，活跃在世界各国，涉及教育、金融、政府等多个行业。国家冲突、奥运会等重要活动期间，DDoS 攻击作为破坏之王，更是成为攻击者手中利刃。数据表明，2021 年 DDoS 攻击频率和强度明显提升，以关键信息基础设施为目标的高强度 DDoS 攻击，已跃升为国家级网络安全威胁之首。

DDoS 攻击如同洪水猛兽，可谓是造成政企业务中断的头号杀手！

中断业务的“三大恶人”之勒索软件

2020 年 4 月底，东京奥运会宣布延期举办约 1 个月后，日本奥委会遭到疑似勒索软件攻击，被迫暂停业务。其秘书处约 100 台服务器中，大约 70% 可能感染病毒的服务器不得不被更换。

勒索凶猛，通过破坏数据的可用性，从而导致业务中断的勒索软件，实际上对业务运行造成的危害与 DDoS 攻击不分伯仲，甚至会直接导致企业倒闭。从发展趋势来看，勒索软件的数量持续上升，攻击面迅速蔓延，同时，由于企业级安全攻击具有高回报率，勒索软件对政府、金融、教育、医疗等多个高价值行业都构成了严重威胁，而这些行业往往与国计民生息息相关。

中断业务的“三大恶人”之挖矿木马

2021 年初，因以比特币为代表的“挖矿”需要耗费巨大的电能，伊朗政府曾指责比特币“挖矿”行为导致

该国电力中断。很多人认为挖矿木马的危害仅仅是让系统变慢，消耗系统资源，不会有破坏性后果。

相较于效果立竿见影的前两种攻击方式，挖矿木马则是瞄准计算机算力逐步蚕食，影响政企机构组织系统运行速度、占用计算机资源，极大可能导致应用程序和硬件崩溃，从而造成业务中断。而其耗费的巨大电能造成的电力中断，又何尝不是一种业务中断?

“三大恶人”的危害之巨，在于通过网络攻击影响行业、国家安全。以防疫时期人人都需要用到的健康码为例，2021 年 5 月，国内某地健康码连续遭受境外网络攻击，严重影响当地出入境秩序。疫情时代下，健康码就是每个人正常工作、生活的出入凭证，一旦健康码系统被黑客攻击，陷入瘫痪状态，影响到绝大多数人的正常出行，后果十分严重。

尤其是在重要时期的网络安全保障，往往也是国内外各类攻击组织最为活跃的时期，大量关键信息基础设施、政企机构内外系统都会成为网络攻击的重要目标。一旦发生恶意破坏、恶意篡改、数据泄露、系统停服等重大网络安全事故，不仅会带来严重的经济损失，也会产生重大的社会影响，防范因网络攻击造成的业务中断更是需要政企考虑的重中之重。

重保就要“零事故” 奇安信推出专项解决方案

面对日益严峻的外部威胁形势，以及重要时期更加频发的安全事件和提升强化的监管力度，政企组织需要应对防范网络安全重大风险、遏制网络安全重大事故的考验，实现不出事故、不被通报，最核心的目标之一就是业务不中断、不延迟。

通过总结、贯彻冬奥“零事故”经验，奇安信推出重保专项解决方案，为政企机构提供重要时期的全方位网络安全保障支撑，协助客户全面深入排查安全隐患，提供 7×24 小时安全监控、事件分析处置和应急响应保障，实现“重保前期控风险清隐患、重保期间强监控‘零事故’”的保障目标，切实提高重要系统运营单位在重要时期的网络安全保障能力。

粉碎“三大恶人”之 DDoS 攻击防御措施

对于 DDoS 攻击、勒索软件和挖矿木马带来的安全威胁，奇安信安全专家提出了更具体、更有针对性的防护建议及相关措施。

针对破坏力极强的 DDoS 攻击，想要完全防住无异于天方夜谭。奇安信安全专家推荐政企客户选择更具针

对性的抗拒绝服务系统（Anti-DDoS）等产品，基于行为异常的攻击检测和过滤机制。产品通过阈值、协议、端口、验证码等多种方式协同保障链路和业务的安全性，防御来自网络层或是应用层的拒绝服务攻击行为，让客户免遭因链路拥塞、服务器资源耗尽，造成业务无法正常运行访问。

粉碎“三大恶人”之勒索软件防御措施

针对来势汹汹的勒索攻击，奇安信安全专家归纳了以下几点建议帮助政企组织有效自救：

首先，要重视常态化安全运营工作。其中包括杜绝使用弱口令，定期开展系统、应用及网络层面的安全评估、渗透测试，以及代码审计工作，主动发现安全隐患，并加强日常安全巡检，定期检查系统配置、网络设备配合、安全日志及安全策略落实情况。

其次，要加强溯源能力，打造体系化和细粒度的安全防护。部署天眼等全流量监测设备、高级威胁监测设备，在服务器上部署安全加固软件，并安装相应的防病毒软件或部署防病毒网关，及时更新、定期扫描。此外，还应加强访问控制 ACL 策略，细化策略粒度。

最后，要提升勒索攻击发生后的快速响应、处置能力。对于已中招的设备下线隔离，使用杀毒软件全面查杀，对于未中招的设备只对特定 IP 开放，尽量关闭高危端口，设置复杂口令。

粉碎“三大恶人”之挖矿木马防御措施

针对特征变化迅速的挖矿木马，奇安信此前曾发布贯穿“边 – 网 – 主机 – 终端”的应对“挖矿”专项方案，从“挖矿”病毒的监测、分析、处置、溯源的闭环处置等进行规划和设计，基于纵深式防护体系构建多重防护机制，结合病毒特性，进行有针对性的多重检测保护，具体措施如下：

其一，在监测和分析环节，主要通过部署天眼，提供威胁情报与威胁监测与分析能力。天眼包括传感器、文件威胁鉴定器（即沙箱系统）、分析平台三大产品设备组件，可提供挖矿病毒专项威胁情报检测、可疑挖矿病毒变种样本分析、未知挖矿病毒异常外联行为检测、挖矿病毒传播过程分析等功能服务。

其二，在处置环节，通过部署椒图，针对操作系统内核、中间件、系统应用进行深层次入侵防护与加固，并结合资产清点、漏扫、风险发现、（挖矿）病毒查杀、基线检查等功能，对攻击行为实施分析、溯源、阻断等措施，对服务器进行从内而外的立体防护；通过部署天擎，有效地对终端进行“挖矿”病毒的查杀与安全加固，提供防护能力，抵御外来的攻击。

同时，客户还可以部署邮件威胁检测系统、DNS 威胁检测系统等，从钓鱼 / 诈骗邮件检测、邮件账号被控、邮箱暴力破解检测，以及恶意域名检测、恶意域名阻断、DNS 隐蔽通道、DGA 域名检测等层面，提供高效的检测和处置方案。

其三，专家服务与安全产品联动。根据天眼、椒图、天擎发现的异常情况和告警，通过奇安信安全服务专家进行安全事件的分析、研判，快速采取相应措施，进行“挖矿”病毒的应急处置。

写在最后

奇安信多年以来持续承接重大活动安全保障任务，经过多年实践，奇安信在重保指挥体系化方面积累了丰富的经验，形成了成熟的一线专家值守、二线应急支撑、三线产品保障及后勤保障的专业重保运营机制。

截至目前，奇安信已先后完成了国庆 70 周年、亚洲文明对话大会、一带一路高峰论坛、海军建军 70 周年、全国两会、春晚、中非合作论坛、上合组织成员国峰会、十九大、博鳌论坛等国家级网络安全保卫任务，用自己的能力和行动捍卫着国家和企业的网络安全。安

奇安信
新一代网络安全领军者

聚焦安全运营，构建智能平台

奇安信网神态势感知与安全运营平台（简称NGSOC）以大数据平台为基础，通过收集多元、异构的海量日志，利用关联分析、机器学习、威胁情报等技术，帮助政企客户持续监测网络安全态势，为安全管理者提供风险评估和应急响应的决策支撑，为安全运营人员提供威胁发现、调查分析及响应处置的安全运营工具。

国内领先的威胁情报能力

奇安信威胁情报中心在情报数量及数据覆盖度方面国内第一。

首款分布式关联分析引擎 - Sabre

国内首款具备分布式关联分析能力的安全运营平台，提供多元异构数据关联分析、灵活威胁建模、丰富的告警上下文信息展示及分布式横向扩展能力，已获得数十个相关专利。

将平战结合进行落地

演练态势监测攻防演练中防守方管理信息、系统建设、威胁运营等信息的总体状况，平战结合，全面提升安全防御能力。

重大安全事件的威胁预警

当出现重大网络安全事件时，帮助用户第一时间掌握是否遭受到攻击？首个被攻击的资产？影响部门？影响面趋势？事件处置情况？

专业的安全运营服务

奇安信集团具有专职产品运营服务团队，可提供原厂一线驻场、二线分析、运营方案咨询及培训服务，帮助客户解决无人运营困难。

市场占有率NO.1

连续2年中国安全管理平台市场占有率第一——赛迪顾问认证
态势感知解决方案市场领导者——IDC认证
态势感知技术创新力和市场执行力双第一 ——数世咨询认证

大事记

中国传媒大学党委书记廖祥忠一行到访奇安信

10 月 19 日，中国传媒大学党委书记廖祥忠一行到访奇安信集团，参观奇安信安全中心展厅、工控实验室、重保指挥中心，并与奇安信安全专家进行交流座谈。

中国传媒大学党委书记廖祥忠表示，奇安信领先的网络安全技术和持续的研发创新能力，特别是对国家的高度责任感令人印象深刻。希望通过和奇安信的深入交流合作，双方共同构建面向国家应用层面的人才培养体系，将网络安全技术与网络强国思想传播深入结合，探索更多合作机遇。

奇安信集团党委书记、董事长齐向东表示，奇安信一直在教育行业深化布局，已同 11 所一流网安学院、20 所 985 重点高校、100 多所本科院校建立了深入合作。此前，奇安信已通过“红色云展厅”项目与中国传媒大学建立了合作，并取得了一定的成果。希望通过未来的深入合作，一方面，共同做好“红色云展厅”项目建设，另一方面，为中国传媒大学实现“三跨越”目标提供全新助力。

共建云上安全生态 奇安信集团与品高股份达成战略合作

10 月 18 日，奇安信集团与品高股份达成战略合作并举行签约仪式。此次战略合作的达成，双方将充分发挥各自在数据、产品、客户资源等方面的优势和能力，联合创新开展技术策源、标准制定、成果转化、解决方案共建等方面的全面战略合作，在复杂的数字化发展机遇中，形成优势互补，共同为各行业客户提供更大的价值服务。

计算机安全专委会党的工作小组成立大会暨与奇安信集团联合党日活动成功举办

10 月 12 日，中国计算机学会计算机安全专业委员会党的工作小组成立大会暨与奇安信集团联合党日活动在奇安信安全中心成功举办。来自公安部、工信部、中国科学院、新华社、国家信息中心、航天科技集团、国家电网，以及国内网络安全头部企业代表参加本次活动。

会议开始前，与会代表在奇安信集团党委书记齐向东的带领下，参观了奇安信集团荣誉展室，并了解集团党建情况。齐向东表示，对于信息化领域工作者来说，必须始终保持强大的战略定力，以党建为引领，把听党话、跟党走当成心里的一杆秤，把站稳政治立场、坚守政治底线当成做事的一把尺，以高度的使命感和责任感开展工作。奇安信也将继续强化党性修养，全力支持、配合专委会党的工作小组工作，推动党建优势进一步转化为发展优势。

根据决议，专委会常务委员、奇安信集团总裁吴云坤担任党的工作小组委员。

奇安信集团与长庆油田达成战略合作 护航数字化转型与智能化发展

10 月 13 日，中国石油天然气股份有限公司长庆油田分公司与奇安信签署战略合作协议。双方围绕网络安全前沿技术研究、网络安全运营、人才培养、安全服务等方面展开深度交流，就共同推进网络安全建设及研究达成战略合作共识。

奇安信与北京轨道交通路网管理有限公司举行数据安全专题交流会

9 月 29 日，北京市基础设施投资有限公司副总经理于增及北京轨道交通路网管理有限公司相关领导到访奇安信，参观奇安信安全中心展厅、工控实验室，并参加了轨道交通行业数据安全专题交流暨冬奥网络安全“零事故”经验分享会。

会上，奇安信安全专家结合冬奥网络安全保障的成果和经验，围绕数安全领域当前面临的变化和挑战，分享了体系化建设思路和工作经验，重点强调了补短板、做好基础安全防护的重要性，并与北京轨道交通路网管理有限公司相关同志，围绕具体应用场景进行了深入交流。

奇安信与重庆市大数据局签署战略合作协议 车联网全国中心落户山城

9 月 27 日，奇安信集团与重庆市大数据发展局签署战略合作协议，双方将在车联网安全、跨境数据安全、数字城市安全领域开展深入合作，共同打造世界级智能网联新能源汽车产业集群、共同服务国际陆海贸易新通道发展。

双方还将共同建设城市安全运营与服务中心，构建面向城市安全的全域安全体系，开展网络安全建设、运行和责任一体化试点，深化网络安全能力建设，服务全市数字经济发展，护航新型智慧城市建设和运行。

奇安信集团与宝兰德达成战略合作 共同打造“安全、可控” 中间件

9 月 26 日，奇安信集团与宝兰德签署战略合作协议，双方将在产品技术能力融合、人才培养、商机拓展、市场活动等方面深度合作。

此前，在 BCS2022 数字安全产业发展论坛上，奇安信与宝兰德及 20 余家生态伙伴共同发起成立“数字产业生态共同体”，共筑“安全基座”，并参与了“安全保发展，发展促安全”主题圆桌对话，围绕数字安全产业发展的特征、机会与生态体系展开深入讨论，为产业发展贡献新视角、新思路。

京东方走进奇安信 参观交流探索安全合作新模式

9 月 23 日，京东方科技集团一行到访奇安信，参观奇安信安全中心展厅、工控实验室，并围绕工控安全、数据安全、供应链安全等领域，与奇安信安全专家进行会谈交流，共同探索平台级、战略级合作新模式。

会上，奇安信安全专家深入分享了冬奥网络安全保障的成果和经验，以及在数据安全、工业互联网安全、供应链安全、终端安全领域的最新成果，与京东方集团 IT、信息安全、数字化相关部门高管进行深入交流，共同探讨网络安全创新合作模式，双方将成立专项组，持续推进相关业务深入开展。

奇安信与中国电信安徽公司签约量子合作项目

9 月 21 日， 2022 量子产业大会在安徽合肥开幕。奇安信集团副总裁陈华平受邀出席大会，并代表奇安信与中国电信安徽公司就量子合作项目进行战略合作签约。

据介绍，本次签约合作的量子加密路由器融合了先进的量子密钥及国密算法，使得数据的安全加密机密性得到极大的增强，让使用量子安全专线的用户业务更加安全。同时，量子加密路由器还继承了奇安信强大的安全基因，在下一代防火墙能力的基础上，还具备 URL 过滤，应用识别，防间谍软件，行为管控等安全能力。

共同构筑石化油服网络安全体系 奇安信与华东石油工程达成战略合作

9 月 20 日，奇安信集团与中石化华东石油工程有限公司达成战略合作协议。双方将在石化行业数字化转型过程中进行网络安全深度合作，包括整体网络安全建设规划、安全运营、前沿技术研究等方面。

本次战略合作的达成，将促进华东石油工程在石化油服体系的信息化安全建设，逐步促进石化油服的网络安全运营中心建设，从管理、技术、制度、流程、人员

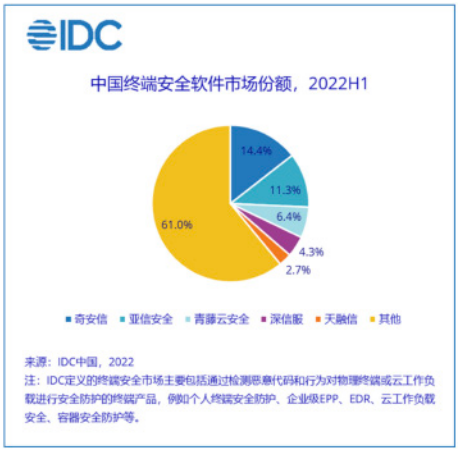
等多方面进行优化及改进。实现石化油服网络完全管理智能化、一体化，实现安全态势全感知、完全风险全预警、安全事件处置全流程。

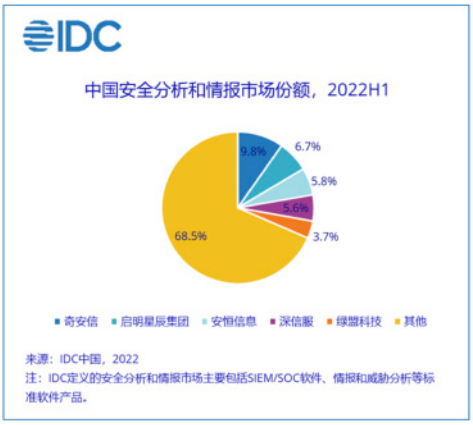
荣誉墙

多年蝉联双冠！奇安信 IT 安全软件市场份额持续领跑

近日，领先的 IT 市场研究和咨询公司 IDC 发布《2022 年上半年中国 IT 安全软件市场跟踪报告》。

《报告》显示，奇安信连续 5 年稳居终端安全软件市场首位，连续 3 年稳居安全分析和情报市场首位，分别实现了市场份额的“五连冠”和“三连冠”。与此同时，奇安信还在首次纳入 IT 安全软件市场研究的信息和数据安全市场排名中位居第二，在国内整体 IT 安全软件市场 7 个领域中，共摘得“两金一银”，整体排名居各大厂商之首。





领域最多！奇安信八大技术入选 Gartner 安全技术成熟度曲线报告

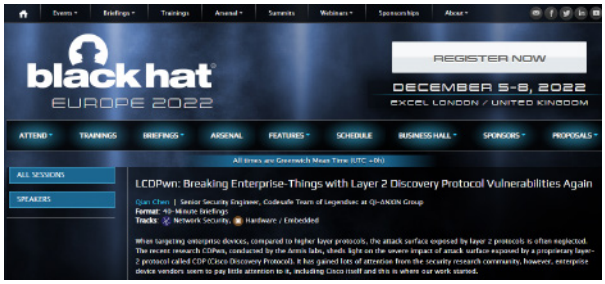
近日，国际权威机构 Gartner 发布《Hype Cycle for Security in China, 2022》，将安全周期划分为技术萌芽期、期望膨胀期、泡沫破裂低谷期、稳步爬升复苏期和生产成熟期五个阶段，涵盖态势感知、零信任、SASE 等十七项技术维度。

其中，奇安信在云安全资源池、智慧城市 CPS 安全、软件成分分析、IoT 身份认证、SASE、态势感知、CWPP 云工作负载保护平台和攻防团队八个维度中被列为代表供应商。

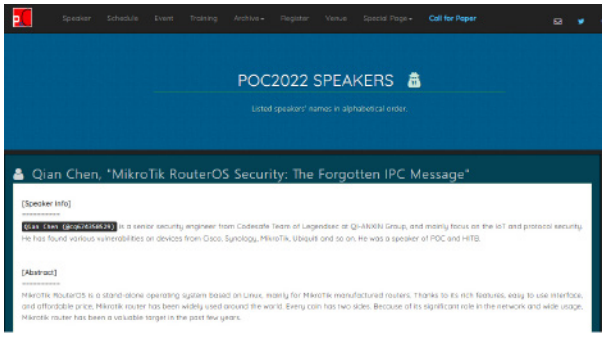
Gartner 在《Hype Cycle for Security in China, 2022》中提到：“安全对于中国的组织来说从未像现在这样重要，尤其是在中国有着严格的法规和法律的情况下。”同时，Gartner 认为：“安全和风险管理领导者应利用这个炒作周期，以获得本地对 IT 创新的观点，并改进其在国内组织的安全控制。”

奇安信代码安全实验室研究成果入选 Black Hat 和 POC 安全大会议题

近日，奇安信代码安全实验室的研究成果 LCDPwn: Breaking Enterprise-Things with Layer 2 Discovery Protocol Vulnerabilities Again 和 MikroTik RouterOS Security: The Forgotten IPC Message，分别入选 2022 年欧洲 Black Hat 安全大会的 Briefings 频道议题和韩国 POC 大会议题。



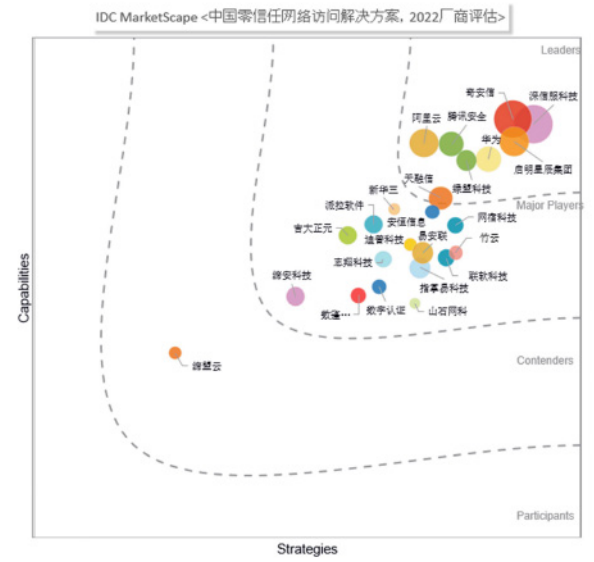
届时，研究员将在 Black Hat 大会上分享如何从 30 个知名厂商的 70 余类设备的 LLDP/CDP 协议解析代码中发现 60 余个安全问题；在 POC 大会上，研究员将关注进程间通信 (IPC) 消息，分享如何通过模糊测试方法来对其健壮性进行测试并最终发现近 60 个漏洞。



牢据领导者位置！奇安信零信任网络访问解决方案再获权威机构认可

IDC 发布了《IDC MarketScape：中国零信任网络访问解决方案，2022 年厂商评估》报告研究，奇安信凭借在零信任市场的技术实力、实践成果、安全生态等多方面领先优势，在入围该报告的厂商中处于领导者位置。

IDC MarketScape: 中国零信任网络访问解决方案，2022



注：请参照附录的详细研究方法，市场定义和评分标准。

来源: IDC, 2022

《报告》介绍，作为 2022 年中国零信任网络访问解决方案厂商领导者，奇安信通过“一中心两体系”内生安全框架将“零信任体系”与“实体安全防护体系”有机结合，实现“主体身份可信、行为操作合规、计算环境与数据实体有效防护”。在北京 2022 年冬奥会和冬残奥会中，奇安信通过零信任身份安全能力支撑服务，为保障“零事故”提供了重要能力。

奇安信获 2022 年度公安部科学技术奖一等奖

近日，公安部公布了 2022 年度公安部科学技术奖励评审结果，由公安部信息安全等级保护评估中心牵头，联合奇安信申报的“关键信息基础设施安全保护关键技术与应用”获得公安部科学技术奖一等奖。

公安部科学技术奖是根据《公安部科学技术奖励办法》，经评审、公示产生，范围涵盖公安各警种和领域，

是公安科技奖励的最高荣誉，代表了公安科技的最高水平。在公安部网络安全保卫局的指导下，评估中心和奇安信联合申报的“关键信息基础设施安全保护关键技术与应用”项目，是首个在关键信息基础设施安全领域获得的一等奖。

奇安信连续 4 年登榜“北京民营企业百强”

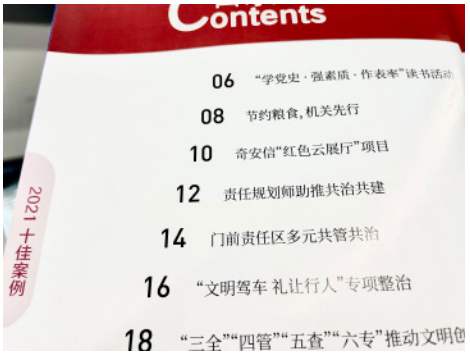
9 月 26 日，北京市工商联召开 2022 北京民营企业百强发布会。奇安信集团连续 4 年入选“民营企业百强”“科技创新”及“社会责任”三大榜单。

据悉，北京民营企业百强调研与发布已连续开展 5 年。通过开展北京民营企业百强调研工作，发现、培育一批引领国内乃至全球行业技术发展的领军企业和符合首都城市功能定位的高成长创新主体。奇安信作为网络安全行业领军企业，已连续 4 年入围百强榜单。

奇安信红色云展厅获评 2021 年“聚力首善共建文明”十佳优秀案例

近日，由首都精神文明建设委员会办公室组织的“2021 年聚力首善 共建文明”主题活动优秀案例正式发布。由市委统战部推荐的奇安信集团“红色云展厅”项目获评 2021 年“聚力首善共建文明”主题活动十佳优秀案例。

2021 年，建党百年之际，奇安信集团联合人民网、中国传媒大学及全国百家红色展馆、数十家省市区广播电视台，共同推出“红色云展厅”。目前，全国已有 237 家展馆加入“红色云展厅”。在人民网微博、微信、党史学习教育官微等平台，“红色云展厅”陆续推出红色场馆文物背后的党史故事，全网总计访问量超过 20 亿，互动量超过 50 万次。



奇安信获 AutoSec 安全之星 2022 年度汽车网络安全突出贡献奖

9 月 21——23 日，AutoSec 2022 第六届中国汽车网络安全周暨汽车数据安全展在上海举行。在“AutoSec Award- 安全之星”年度行业评选中，奇安信集团获得“AutoSec Awards 安全之星” 2022 年度汽车网络安全突出贡献奖。

作为国内历时最久、最有影响力的行业品质会议之一，中国汽车网络安全周一直专注于汽车网络信息安全。经过多轮投票，凭借在车联网安全行业的突出贡献和杰出实力，奇安信集团获评“AutoSec Awards 安全之星”2022 年度汽车网络安全突出贡献奖。

奇安信
新一代网络安全领军者

聚焦安全运营，构建智能平台

奇安信网神态势感知与安全运营平台（简称NGSOC）以大数据平台为基础，通过收集多元、异构的海量日志，利用关联分析、机器学习、威胁情报等技术，帮助政企客户持续监测网络安全态势，为安全管理者提供风险评估和应急响应的决策支撑，为安全运营人员提供威胁发现、调查分析及响应处置的安全运营工具。

国内领先的威胁情报能力

奇安信威胁情报中心在情报数量及数据覆盖度方面国内第一。

首款分布式关联分析引擎 - Sabre

国内首款具备分布式关联分析能力的安全运营平台，提供多元异构数据关联分析、灵活威胁建模、丰富的告警上下文信息展示及分布式横向扩展能力，已获得数十个相关专利。

将平战结合进行落地

演练态势监测攻防演练中防守方管理信息、系统建设、威胁运营等信息的总体状况，平战结合，全面提升安全防御能力。

重大安全事件的威胁预警

当出现重大网络安全事件时，帮助用户第一时间掌握是否遭受到攻击？首个被攻击的资产？影响部门？影响面趋势？事件处置情况？

专业的安全运营服务

奇安信集团具有专职产品运营服务团队，可提供原厂一线驻场、二线分析、运营方案咨询及培训服务，帮助客户解决无人运营困难。

市场占有率NO.1

连续2年中国安全管理平台市场占有率第一——赛迪顾问认证
态势感知解决方案市场领导者——IDC认证
态势感知技术创新力和市场执行力双第一 ——数世咨询认证

奇安信 BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

网络安全 中国代表队 | 奇安信

2022年北京冬奥会胜利闭幕

“零事故”

奇安信圆满完成冬奥会网络安全保障任务

奇安信蝉联“中国网安产业竞争力50强”第一名

6月23日，中国网络安全产业联盟（CCIA）
揭晓“2022年中国网安产业竞争力50强”榜单。
凭借在网络安全领域领先的技术实力以及突出的市场表现，
奇安信蝉联第一名。


奇安信科技集团股份有限公司

CCIA 50强

2022年中国网安产业竞争力50强

编号：CCIA-2022JZL-01

中国网络安全产业联盟
2022年6月

“2022年中国网安产业竞争力50强”榜单

TOP15	公司名称
1	**奇安信科技集团股份有限公司**
2	深信服科技股份有限公司
3	启明星辰信息技术集团股份有限公司
4	天融信科技集团股份有限公司
5	华为技术有限公司
6	绿盟科技集团股份有限公司
7	腾讯云计算（北京）有限责任公司
8	阿里云计算有限公司
9	新华三技术有限公司
10	杭州安恒信息技术股份有限公司
11	360政企安全集团
12	亚信安全科技股份有限公司
13	成都卫士通信息产业股份有限公司
14	杭州迪普科技股份有限公司
15	山石网科通信技术股份有限公司