极牛网络安全通讯 • 社群期刊

2024 年 11 月 第 41 期

网安观察

第41期

2024年11月

CONTEN

目录

安全态势

国际视野

CONTENTS

专题报道

第 41 期

《网安观察》编辑部

主办　极牛网

总　　编　　辑：陈鑫杰
总　　顾　　问：叶绍琛
副　　总　　编：王文彦
威胁情报主编：陈艇鑫
移动安全主编：蔡国兆
网安人才主编：林俊濠
涉网犯罪主编：胡铭凯
网安产业主编：张九史
网安态势主编：郑泽彬

公众号　小程序　网站

电子版请访问　www.geeknb.com　阅读或下载索阅、投稿、建议和意见反馈，请联系极牛网期刊编辑部。

E m a i l：hi@geeknb.com
地　　址：深圳市龙岗区天安云谷2栋2层
邮　　编：518000
电　　话：0755-33228862
印刷数量：1000 本
印刷单位：深圳彩虹印刷有限公司

政策篇

国内，行业数据安全政策标准不断推进。《反洗钱法》修订加强数据保护，《金融数据安全治理实施指南》等 3 项数据安全标准获批发布，工信部印发《工业和信息化领域数据安全事件应急预案（试行）》，国家数据局《可信数据空间发展行动计划（2024—2028 年）》公开征求意见；

国际上，美国收紧敏感数据跨境流通规则，司法部、网络安全与基础设施安全局先后发布数据安全拟议新规，以防止外国获取敏感数据。美国联邦 IT 领导层还发布了《联邦零信任数据安全指南》，推动以数据为中心的保护理念。

国内

《反洗钱法》修订表决通过，更好地保护数据安全和公民个人信息

11 月 8 日，十四届全国人大常委会第十二次会议表决通过了新修订的反洗钱法，自 2025 年 1 月 1 日起施行。为了更好地保护数据安全和公民个人信息，修订后的反洗钱法作了多方面规定。一是在保留现行反洗钱法关于严格规范反洗钱信息使用规定的同时，增加了规定对个人隐私的保护。二是明确要求提供反洗钱服务的机构及其工作人员对于因提供服务获得的数据、信息，应当依法妥善处理，确保数据、信息安全。三是增加规定金融机构在公司内部、集团成员之间共享反洗钱信息，也应当符合有关信息保护的法律规定。四是增加规定有关国家机关工作人员泄露反洗钱信息的法律责任。

《网络安全技术 终端计算机通用安全技术规范》等 3 项国家标准获批发布

11 月 5 日，根据 2024 年 10 月 26 日国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告（2024 年第 24 号），全国网络安全标准化技术委员会归口的 3 项网络安全国家标准正式发布。具体包括《网络安全技术 终端计算机通用安全技术规范》《网络安全技术 存储介质数据恢复服务安全规范》《网络安全技术 网络弹性评价准则》。

住房城乡建设部印发《城市数字公共基础设施标准体系》

11 月 1 日，住房城乡建设部组织编制了《城市数字公共基础设施标准体系》，为城市实现数字化转型发展提供统一数字底座，并对接底座一体化推进城市数字应用体系建设。该文件提出，城市数字公共基础设施标准体系框架分为九类，其中安全与保障类主要规范信息技术应用创新、安全与保障等方面的要求，包括网络安全、数据安全、密码应用安全和其他 4 个子类标准。

工信部印发《工业和信息化领域数据安全事件应急预案（试行）》

10 月 31 日，工业和信息化部印发《工业和信息化领域数据安全事件应急预案（试行）》，以建立健全工业和信息化领域数据安全事件应急组织体系和工作机制，提高数据安全事件综合应对能力。该文件共八部分，包括总则、组织体系、监测与预警、事件响应、事后总结、预防措施、保障措施、附则。该文件将数据安全事件分为特别重大、重大、较大和一般四个级别。地方行业监管部门认为可能发生重大及以上数据安全事件的，应当立即上报工信部数据安全机制；工业和信息化领域数据处理者、数据安全应急支撑机构认为可能发生较大及以上数据安全事件的，应当立即向地方行业监管部门报告。

三部门印发《新材料大数据中心总体建设方案》

10 月 30 日，工业和信息化部、财政部、国家数据局联合印发《新材料大数据中心总体建设方案》，以充分发挥大数据、人工智能对新材料产业的技术支撑作用，培育材料研发与应用的全新发展模式。该文件提出，计划到 2027 年，搭建形成“1+N”（1 个中心主平台、N 个数据资源节点）的新材料大数据中心架构体系。该文件要求，完善数据安全管理技术标准规范，强化对新技术新应用的数据安全风险研究和评估，建立数据安全保障体系，研发安全可靠的关键技术和软件，并实施应用示范。

中国互联网金融协会发布《金融数据安全治理实施指南》等 3 项数据安全标准

10 月 25 日，中国互联网金融协会在京召开金融数据安全治理工作研讨会暨金融数据安全系列标准发布会，正式发布了《金融数据安全治理实施指南》《金融数据安全技术防护规范》《金融数据安全应急响应和处置指引》等 3 项标准，旨在从金融数据治理、金融数据安全技术防护、金融数据安全应急管理等不同角度，为做好新时代的金融数据安全治理工作提供相应指引和规范。

国家数据局《可信数据空间发展行动计划（2024—2028 年）》公开征求意见

10 月 18 日，国家数据局研究起草了《可信数据空间发展行动计划（2024—2028 年）》，现向社会公开征求意见。该文件指出，可信数据空间是基于共识规则，联接多方主体，实现数据资源共享共用的数据流通利用基础设施。该文件在安全保障方面提出加强两方面能力，一是安全防护能力，可信数据空间应针对数据流通的全生命周期，构建必要的防范和检测技术手段，防止数据泄露、窃取、篡改等危险行为发生，并建立相关的管理制度和应急处置措施；二是合规监管能力，可信数据空间应监测空间中违反相关法律法规的行为，并应在行为发生时，及时采取相应的处置措施。

国际

美国 NIST 发布后量子密码迁移路线图公开草案

11 月 12 日，美国国家标准与技术研究院（NIST）发布了《过渡到后量子密码学标准》初始公开草案，包含迁移的路线与时间表。根据草案，NIST 希望到 2035 年将政府机构的加密系统转变为后量子加密，该机构将在 2030 年前弃用 112 位及以下安全强度的加密算法，于 2035 年前禁用这些算法。NIST 指出，向后量子密码学迁移的初期可能会采用混合解决方案，这些方案在建立加密密钥或生成数字签名时结合了抗量子算法和易受量子攻击算法的使用，以确保至少一个算法安全时整体系统的安全性。

美国运输安全管理局发布拟议规则，要求管道和铁路公司必须建立网络风险管理计划

11 月 6 日，美国运输安全管理局发布《加强地面网络风险管理》拟议规则，要求部分铁路、轨道交通和管道等地面运输系统的所有者和运营者执行网络风险管理和事件报告要求。该文件沿袭了运输安全管理局 2021 年以来年度安全指令的基于绩效的网络安全要求，并基于 NIST 网络安全框架、CISA 跨部门网络安全绩效目标等成果，主要提出三方面要求，一是建立健全网络风险管理计划，二是向 CISA 报告网络安全事件，三是指定一名物理安全协调员专门向运输安全管理局报告重大物理安全问题。该文件将在 2025 年 2 月 5 日截止征求意见。

德国司法部发布计算机刑法修正草案，保护白帽黑客行为

11 月 4 日，德国联邦司法部发布计算机刑法修正草案公正征求意见，明确研究 IT 安全漏洞的法律责任。该文件主要提出了两方面修改，一是将发现安全漏洞行为排除犯罪，确

保发现并负责任报告安全漏洞的研究人员，不会有承担刑事责任的风险；二是加大对网络间谍活动的处罚，如刺探和拦截数据符合特别严重案件标准或导致德国关键基础设施、国家安全受到损害，可处以 3 个月到 5 年有期徒刑。德国联邦司法部长 Marco Buschmann 博士表示：“那些致力于弥补 IT 安全漏洞的人，应该得到的是表彰，而不是检察官的诉讼通知。”此前美国、欧洲比利时、马其他等国均有修订法律，对白帽黑客行为可豁免起诉。

美国政府发布《联邦零信任数据安全指南》

10 月 31 日，美国联邦首席数据官委员会、联邦首席信息安全官委员会等联邦政府 IT 领导层联合发布了《联邦零信任数据安全指南》，旨在强化数据安全实践。该文件共 42 页，重点强调了“保护数据本身，而非保护数据的边界”。官方认为这一理念是“有效实施零信任的基础支柱”之一。该文件提出了 5 个步骤的零信任安全路线图，概述了实践者可以采取的具体行动，包括发现、清点、分类、标记和映射数据流，进行风险分析，与零信任架构对齐，设计控制和监控，拥抱自动化和编排。

美国网络安全与基础设施安全局发布首部国际战略规划

10 月 29 日，美国网络安全与基础设施安全局（CISA）发布了《2025–2026 财年 CISA 国际战略规划》，旨在将加强国际伙伴关系作为全球竞争的“力量倍增器”，使美国能够在当前和未来竞争并战胜全球范围内的威胁和挑战，实现该机构为美国民众提供安全和有弹性的基础设施的愿景。该文件列出了 CISA 必须实现的三项目标，以应对美国及其国际伙伴面临的不断变化和动态的挑战。一是增强美国所依赖的外国基础设施的弹性；二是加强国际伙伴关系，促进美国关键基础设施的优先发展和海外利益；三是制定操作和技术全球标准、法规、政策、指南和最佳实践，以提高安全性。

美国财政部发布对外投资审查最终规则

10 月 28 日，美国财政部发布了一项最终规则，以实施拜登于 2023 年 8 月发布的第 14105 号行政命令（Reverse CFIUS 行政令）。根据该行政令的规定，最终规则禁止美国公民参与涉及特定技术和产品的某些交易，还要求美国公民通报涉及特定技术和产品的某些其他交易。涵盖的特定技术和产品分为三类：半导体和微电子、量子计算、人工智能。拜登政府认为这些技术是下一代军事、网络安全、监视和情报应用的核心。美国发布对外投资审查的新计划是对现有出口管制和投资审查工具的补充，试图阻止美国资本推动受关注国家敏感技术和产品的开发。最终规则将中华人民共和国、中国香港特别行政区及中国澳门特别行政区均列为受关注国家和地区。该规则将于 2025 年 1 月 2 日生效。

美澳网络安全监管机构发布软件安全部署指南

10 月 24 日，美国网络安全与基础设施安全局、联邦调查局及澳大利亚信号局旗下网络安全中心联合发布《安全软件部署：软件制造商如何确保对客户的可靠性》，以支持软件制造商实施具备健壮测试和测量组件的软件安全部署流程。该文件概述了软件安全部署的六个关键阶段，包括规划、开发和测试、内部推广、部署和小规模测试、受控推广、将反馈意见纳入规划。该文件强调创建和维护剧本（Playbook），为每个部署阶段提供明确的指导方针、最佳实践和应急计划。

美国政府发布首份关于人工智能的国家安全备忘录

10 月 24 日，美国白宫公开发布首份关于人工智能的国家安全备忘录，旨在确保美国在抓住人工智能机遇和管理人工智能风险方面发挥领军作用，鼓励联邦政府采用人工智能来推进国家安全使命，并寻求塑造围绕人工智能使用的国际规范。除了该备忘录，美国白宫还发布了《国家安全领域推进人工智能治理和风险管理框架》，对此前针对非国家安全任务的指南进行了补充。该框架提供了实施备忘录的进一步细节和指导，包括要求建立风险管理、评估、问责和透明度机制。

美国 CISA 发布数据安全拟议新规，防止外国获取敏感数据

10 月 21 日，根据美国总统拜登 2 月签署的第 14117 号行政命令《关于防止受关注国家获取美国人大量敏感个人数据和美国政府相关数据的行政命令》，美国网络安全与基础设施安全局（CISA）发布拟议实施文件公开征求意见。该文件主要针对参与受限交易领域的企业，特别是那些可能持有、处理大量美国政府和公民敏感数据，提出了多项安全措施。该文件提出了一系列组织级别与数据级别的具体要求，包括维护资产清单、漏洞修补、网络拓扑维护、多因素认证、数据加密与脱敏、限制未授权硬件连接等。

美国司法部发布拟议新规，防止外国获取敏感数据

10 月 21 日，美国司法部公布了《应对美国敏感数据面临的国家安全风险拟议规则》（NPRM），并再次征求公众意见。该项拟议规则以今年 2 月美国总统签署第 14117 号行政命令后司法部同日制定的拟议规则预通知（ANPRM）为基础。NPRM 在分析对 ANPRM 的相关公众反馈后再次对外发布，以解决美国人的敏感数据和政府相关数据，被包括中国在内的“关注国、地区、个人”获取的国家安全威胁。该文件定义了六类美国人敏感数据和两类美国政府敏感数据，将禁止数据经纪公司与关注国进行敏感数据交易、限制与敏感数据相关的投资和合作协议、实施数据交易记录和审查机制。

欧盟委员会通过 NIS2 指令首个实施条例

10 月 17 日，欧盟委员会根据《关于在欧盟实现高度统一网络安全措施的指令》（NIS2 指令），通过了有关关键实体和网络安全的首个实施条例。实施条例将适时在欧盟官方公报公布，并于 20 天后生效。该文件针对 DNS、TLD 域名注册、云服务、数据中心、CDN、托管服务、托管安全服务、在线市场、搜索引擎、社交网络服务、信托服务等提供商，提出了网络安全风险管理措施的技术和方法要求。该文件定义了构成重大事件的具体情形，并要求提供数字基础设施和服务的公司应履行向国家当局报告的义务。

新加坡网络安全局发布《AI 系统安全指南》

10 月 15 日，新加坡网络安全局发布了《AI 系统安全指南》《AI 系统安全配套指南》两份文件，以帮助 AI 系统所有者在全生命周期内保护 AI。这两份文件将有助于保护 AI 系统，免受供应链攻击等传统网络安全风险和对抗性机器学习等新风险的影响。其中，《AI 系统安全配套指南》是一份社区合作编写的参考文件，从工业和学术界精选了实用的措施、安全控制和最佳实践。这两份文件将动态更新，以反映该领域的最新发展。

美国防部发布网络安全成熟度模型认证计划最终规则

10 月 11 日，美国防部发布网络安全成熟度模型认证（CMMC）计划最终规则。该规则将评估级别从原来的 5 个减少至 3 个，并允许企业视情况对其合规性进行自我评估，以简化中小企业合规成本。联邦合同信息（FCI）的基本保护将需要 CMMC1 级的自我评估；受控非机密信息（CUI）的一般保护将需要第三方评估或 CMMC2 级的自我评估；部分需要更高级别保护，以防范 APT 风险的 CUI，需要由国防工业基础网络安全评估中心牵头进行 CMMC3 级评估。

欧盟理事会通过《网络弹性法案》

10 月 10 日，欧盟理事会宣布通过《网络弹性法案》，以保护欧盟的所有数字产品免受网络威胁。《网络弹性法案》是全球首个数字产品安全立法，它对所有硬件和软件设置了不同级别的强制性网络安全要求，制造商需要在产品生命周期内实施对应措施，并附带 CE 标志表明符合法律要求，才可以在欧盟销售。该法案已于 3 月 12 日经欧洲议会批准通过，下一步需欧盟理事会主席和欧洲议会主席签署发布才能成为法律。

事件篇

国内网络安全执法日益增多。大量个人信息数据遭境外访问窃取，上海某医疗科技企业被行政处罚；河南两公司泄露大量敏感数据被罚 10 万元；国家安全部披露，某境外企业“借壳”国内测绘企业非法窃取测绘地理信息被罚。

25 家跨国企业数据泄露，MOVEit 漏洞引发重大安全危机

11 月 11 日 Infostealers 消息，网络犯罪情报厂商 HudsonRock 发布报告称，一名昵称为“Nam3L3ss”的黑客 8 日在地下论坛发布了利用 MOVEit 漏洞（CVE-2023-34362）获取的大量企业员工数据，据称来自麦当劳、汇丰、亚马逊、联想、惠普等多家知名跨国企业，如涉及亚马逊超 286 万条记录、大都会人寿超 58 万条记录、汇丰银行超 28 万条记录等。此次被公开泄漏的被盗数据包括来自 25 家跨国企业的员工详细信息，如姓名、邮箱地址、电话号码、成本中心代码和组织结构等。这次泄密事件再次凸显了 MOVEit 漏洞的深远影响，以及未迅速应用安全补丁所带来的风险。

美国知名军工芯片厂商因勒索攻击损失超 1.5 亿元

11 月 6 日 SecurityWeek 消息，美国知名军工半导体厂商微芯科技（Microchip）5 日发布最新财报披露，因近期网络安全事件，公司已产生 2140 万美元（约合 1.53 亿元人民币）的相关费用。此次事件在 8 月首次曝光，当时微芯科技发现其网络系统中出现了可疑活动，并直接导致公司部分制造设施的生产中断。大约一周后，勒索软件团伙 Play 宣称对此次攻击负责。该团伙公布了一个 4GB 大小的压缩文件，声称其中包含微芯科技的内部数据。这些数据包括个人信息、客户文件及与预算、工资、会计、合同、税务和财务等相关的文件。9 月初，在恢复大部分运营后，微芯科技确认，威胁行为者确实从其系统中窃取了一些信息，其中包括员工的联系方式和密码哈希值。

国际石油巨头哈里伯顿因网络攻击损失超 2.5 亿元

11 月 8 日 Cybersecurity Dive 消息，美国石油巨头哈里伯顿（Halliburton）首席执行官 Jeff Miller 在季度财报电话会议上表示，8 月的网络攻击及墨西哥湾风暴导致收入损失或延迟，致使公司调整后每股收益减少了 2 美分。公司财报显示，此次网络攻击直接带来了约 3500 万美元（约合 2.51 亿元人民币）相关费用。公司表示，此次入侵迫使其推迟账单和收款，对当季现金流造成了影响，但不构成重大影响。这次攻击被怀疑与 RansomHub 威胁组织有关，该组织是今年全球最为活跃的黑客团体之一。

施耐德电气遭数据勒索：开发平台访问凭证暴露 40GB 数据失窃

11 月 4 日 BleepingComputer 消息，能源管理巨头施耐德电气确认，内部一个开发平台遭入侵。此前有威胁行为者声称，利用暴露的凭证从该公司 JIRA 服务器窃取了 40GB 数据，并威胁索要价值 12.5 万美元的赎金。施耐德电气表示：“公司正在调查一起网络安全事件，涉及未经授权访问我们内部的项目执行跟踪平台之一，该平台位于一个隔离的环境中。公司全球事件响应团队已立即动员应对此事件。施耐德电气的产品和服务未受到影响。”

德国大型药品批发商遭勒索攻击，欲扰乱超 6000 家药房供应

11 月 1 日 GovinfoSecurity 消息，德国药品批发商 AEP 在 10 月 28 日遭遇勒索软件攻击，部分 IT 系统被加密，通信系统也受到影响，无法处理订单，导致供应链中断，只能向药店提供有限范围的供货。AEP 负责向全德境内 6000 多家药房供应药品，据悉，目前尚未导致药品短缺。巴伐利亚药剂师协会表示，巴伐利亚州的药品供应不存在风险，药房通常会多家批发商合作。

墨西哥大型机场集团疑遭勒索攻击，旗下 13 个机场紧急切换备用系统

10 月 26 日 The Record 消息，墨西哥中北部机场集团（OMA）25 日披露，一起网络事件迫使其 IT 团队切换至备份系统，以维持墨西哥中部和北部 13 个机场的正常运营。24 日，RansomHub 勒索软件组织宣称对此次攻击负责，并威胁如果不支付赎金，他们将公开 3TB 的被盗数据。具体的赎金金额尚不清楚。此次网络攻击影响超 10 天，OMA 15 日在社交平台上首次承认了此次事件，表示旗下各机场的大屏已经关闭，目前仍只能通过备用系统和人工服务维持运营。

通过外网非法获取公民个人信息 1 亿余条，一安全公司员工获刑

10 月 28 日澎湃新闻消息，上海市杨浦区人民检察院召开新闻发布会，通报 2020 年以来侵犯公民个人信息隐私案件办理情况，并发布相关案例。其中一起通报案例显示，被告人吴某是某安全科技有限公司员工。2024 年 2 月，被告人吴某通过翻墙软件违规访问境外 Telegram 平台，并在该软件“ling 某”群的“资源共享”内下载含有公民个人信息的文件，储存在其持有的移动硬盘中，同时将上述下载渠道提供给他人。经鉴定，被告人吴某非法获取的公民个人信息共计 1 亿余条。经杨浦区检察院提起公诉，法院以侵犯公民个人信息罪判处吴某有期徒刑一年六个月，缓刑一年六个月，并处罚金 2000 元人民币。

近年最大规模！超 1 亿美国人医疗隐私数据被盗

10 月 24 日 BleepingComputer 消息，美国联合健康集团首次确认，由于旗下子公司 Change Healthcare 遭遇勒索软件攻击，超过 1 亿人的个人信息和医疗数据被盗。此次事件已成为近年来最大规模的医疗数据泄露事件。美国卫生与公共服务部民权办公室 24 日在其数据泄露门户网站上更新了受影响人数的统计，总人数为 1 亿人。这是联合健康集团首次为此次数据泄露事件提供官方数字。在民权办公室网站更新的常见问题解答中写道：“2024 年 10 月 22 日，Change Healthcare 向民权办公室报告，已向约 1 亿人发出了个人通知，告知他们此次数据泄露事件。”据悉，被窃取的数据包括健康保险信息、医疗诊断信息、账单索赔与支付信息、其他个人信息等。

河南两公司泄露大量敏感数据被罚 10 万元

10 月 23 日网信郑州消息，郑州市网信办工作中发现，该市两家公司未履行网络安全保护义务，未采取必要的安全防护，导致大量敏感数据被窃取。经调查核实，公司一在数据库中配置增加了远程登录空口令账户，导致黑客利用该空口令账户成功登录数据库，并窃取了数据库中的数据，被窃取的数据包括姓名、身份证号、手机号、邮箱地址等敏感信息。公司二缺乏网络安全意识，没有正确配置数据库，导致数据库存在未授权访问漏洞，攻击者通过漏洞登录数据库，查看、下载数据，导致敏感数据泄露。郑州市网信办依据《数据安全法》分别对两家公司作出责令改正，并给予警告，处以人民币 5 万元罚款的行政处罚。

国家网络安全通报中心：多个与某大国政府有关的境外黑客组织持续攻击国内单位企业

10 月 21 日国家网络安全通报中心消息，中国国家网络与信息安全信息通报中心发现一批境外恶意网址和恶意 IP，有多个具有某大国政府背景的境外黑客组织，利用这些网址和 IP 持续对中国和其他国家发起网络攻击。这些恶意网址和

IP 都与特定木马程序或木马程序控制端密切关联，网络攻击类型包括建立僵尸网络、网络钓鱼、勒索病毒等，以达到窃取商业秘密和知识产权、侵犯公民个人信息等目的，对中国国内联网单位和互联网用户构成重大威胁，部分活动已涉嫌刑事犯罪。相关恶意网址和恶意 IP 归属地主要涉及：美国、波兰、荷兰、保加利亚、土耳其、日本等。

卡西欧遭遇灾难式勒索攻击：系统瘫痪、交付延迟、财报推迟

10 月 21 日 The Record 消息，日本知名手表制造商卡西欧计算机株式会社宣布，由于 10 月 5 日发生的勒索软件攻击影响了公司的会计流程，原定于 11 月 6 日发布的第二季度财报将推迟至 11 月中旬。该公司官网声明称，此次攻击导致“交货日期严重推迟，并积压了大量维修请求。公司目前正全力应对这一情况，计划在 11 月底之前恢复系统的正常运行”。“Underground”勒索软件团伙声称对这次攻击负责。该组织称他们窃取了公司 204.9 GB 的数据，并发布了部分被盗数据作为证据。

上市公司科沃斯旗下扫地机器人被黑并发出骚扰声：用户受惊 官方回应

10 月 13 日 The Verge 消息，澳媒 ABC 新闻日前报道称，今年 5 月，黑客获取了科沃斯地宝 X2 Omni 扫地机器人在多个美国城市的控制权，利用这些机器人追赶宠物并向主人大喊种族歧视性言论，明尼苏达州、埃尔帕索、洛杉矶等多地均有用户反馈。科沃斯公司随后对此声明称，经调查，他们确认了一次“凭证填充攻击”事件，并已屏蔽了相关的 IP 地址。公司强调，目前“没有证据显示”攻击者获得了用户的用户名和密码。

国家安全部：某境外企业“借壳”国内测绘企业非法窃取测绘地理信息

10 月 16 日国家安全部公众号消息，国家安全部公众号发文称，国家安全机关工作发现，某境外企业 A 公司通过与我国具有测绘资质的 B 公司合作，以开展汽车智能驾驶研究为掩护，在我国内非法开展地理信息测绘活动。为尽可能直接获取原始测绘数据，A 公司越过项目转包的层层节点，全程主导测绘项目进展，直接指挥 B 公司人员在我国内多省份开展测绘，更是专门委派外籍技术专家对 B 公司的测绘人员开展实操指导，重点把控测绘数据的存储、处理和流转等环节。最后在 A 公司的操控指使下，B 公司将测绘所得数据转移出境。经鉴定，A 公司采集的数据多项属于国家秘密。在此事件中，B 公司开展测绘活动时忽视了测绘行业相关规定要求，任由境外企业把控数据流向，导致原始测绘数据失控外传。针对以上情况，国家安全机关会同有关部门开展了联合执法活动。涉事企业和有关责任人受到了法律追究。

大量个人信息数据遭境外访问窃取，上海某医疗科技企业被行政处罚

10 月 14 日网信上海公众号消息，上海市网信办接到线索，反映属地某医疗科技公司所属系统存在网络安全漏洞，致使系统大量个人信息数据发生泄漏被境外 IP 访问窃取。通过调查核实，涉事系统为该企业内部生产测试系统，部署于云服务平台，系统数据库内存储大量个人信息数据，包含姓名、单位名称、所属省市、所在乡镇 / 街道、手机号（已采取加密措施）等。该系统未采取有效网络安全防护措施，存在未授权访问漏洞，网络和数据安全管理制度不完善，网络日志留存不足 6 个月，造成数据泄漏被窃取，违反了《数据安全法》第二十七条规定。针对以上违法情况，上海市网信办依据《数据安全法》第四十五条规定对该医疗科技公司给予警告，并处以罚款的行政处罚。

伊朗政府部门和核设施遭受大规模网络攻击

10 月 12 日 Security Affairs 消息，伊朗遭受大规模网络攻击，导致伊朗政府服务中断、重要信息被窃取，尤其是核设施也受到了影响。伊朗最高网络安全委员会前秘书菲鲁扎巴迪表示，此次网络攻击影响了伊朗政府内部的关键部门，包括司法、立法和行政部门，大量重要信息也因此被窃取；伊朗的核设施及燃料分配、市政服务、交通和港口的关键网络也成为攻击目标。此次网络攻击被视为以色列对伊朗本月早些时候导弹袭击的可能报复，加剧了两国间持续的紧张局势，可能引爆更大范围的冲突。

漏洞篇

Web 控制面板开源项目 CyberPanel 曝出高危漏洞，可未授权远程执行任意命令。该漏洞技术细节和 EXP 均公开且可复现，测绘数据显示国内上万资产受影响，建议客户尽快做好自查及防护。

CyberPanel 远程命令执行漏洞安全风险通告

10月28日，奇安信CERT监测到官方修复CyberPanel upgrademysqlstatus 远程命令执行漏洞（QVD-2024-44346），该漏洞源于 upgrademysqlstatus 接口未做身份验证和参数过滤，未授权的攻击者可以通过此接口执行任意命令获取服务器权限，从而造成数据泄露、服务器被接管等严重的后果。奇安信鹰图资产测绘平台数据显示，该漏洞关联的国内风险资产总数为12,289个，关联IP总数为4316个。目前该漏洞技术细节与 EXP 已在互联网上公开，奇安信威胁情报中心安全研究员已成功复现，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 FortiManager 身份认证绕过漏洞在野利用通告

10 月 24 日，奇安信 CERT 监测到官方修复 Fortinet FortiManager 身份认证绕过漏洞（CVE-2024-47575），未经身份验证的远程攻击者可以使用有效的 FortiGate 证书在 FortiManager 中注册未经授权的设备。成功利用漏洞后攻击者将能够查看和修改文件（如配置文件）以获取敏感信息，并能够管理其他设备执行任意代码或命令。奇安信鹰图资产测绘平台数据显示，该漏洞关联的国内风险资产总数为 39,073 个，关联 IP 总数为 39,674 个。鉴于此漏洞已发现在野利用，建议客户尽快做好自查及防护。

Spring Framework 路径遍历漏洞安全风险通告

10 月 18 日，奇安信 CERT 监测到官方修复 Spring Framework 路径遍历漏洞（CVE-2024-38819），在 Spring Framework 受影响版本中，当应用程序使用 WebMvc.fn 或 WebFlux.fn 提供静态资源时，容易受到路径遍历攻击。攻击者可以编写恶意 HTTP 请求并获取目标系统上任何由 Spring 应用程序正在运行的进程访问的文件，从而导致信息泄露。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

Apache Solr 身份认证绕过漏洞安全风险通告

10 月 16 日，奇安信 CERT 监测到官方修复 Apache Solr 身份认证绕过漏洞（CVE-2024-45216），该漏洞存在于 Apache Solr 的 PKIAuthenticationPlugin 中，该插件在启用 Solr 身份验证时默认启用。攻击者可以利用在任何 Solr API URL 路径末尾添加假结尾的方式，绕过身份验证访问任意路由，从而获取敏感数据或进行其他恶意操作。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

红帽人才工程

Cyber Crime Governance Talent Training Project

工程简介

在“全国网络警察培训基地”的指导下，中国下一代网络安全联盟牵头发起「红帽人才工程」，联合华云信安、美亚柏科、高联通信等知名网络安全企业，围绕“网络犯罪治理、涉网犯罪打击”等相关网络安全课题，持续挖掘、培养、资助、赋能网络安全人才，构建红色基因的网络空间安全人才防线。

申报流程

课题征集 → 课题公示 → 立项评审

研究课题计划征集

研究课题信息公示

研究课题立项评审

申报说明

项目资讯

培养对象

政企单位在职人员、高校全日制在校生（含研究生）、互联网企业技术人员、网络安全企业技术人员以及社会网络安全人才...

核心课题

内网攻防、社工钓鱼、远控木马、免杀加壳、情报甄别、资金分析、调证溯源、取证固证、远程勘验、APP反编译、二进制逆向...

特朗普 2.0
网络安全迎来哪些巨变？

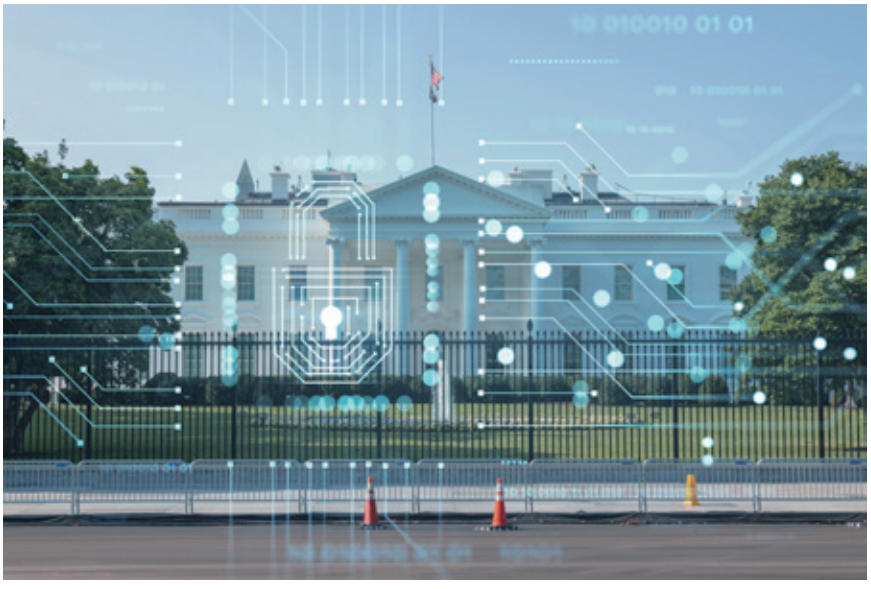
特朗普第二任期网安政策迎来五大变化

特朗普和拜登的执政理念大相径庭，重返白宫的特朗普在网络安全政策方面会有哪些变化？是否会接受拜登的“网络安全遗产”？这是全球网络安全行业当下最为关心的话题之一。

网络安全是少数几个得到美国共和与民主两党支持的领域。穆迪评级承认美国两党的网络政策在很多方面是相同的，但同时也认为，关键的政策差异可能会导致发生重大变化。

安全专家预测，特朗普可能会对现有的网络安全政策进行调整，以突出其一贯的“灵活响应、减少监管”策略。

- 保留和强化对关键基础设施和联邦网络防护措施，但减少对私营企业的过多监管。
- 继续加大防御投入，推进网络现代化进程，部署“所有工具”保护关基安全。
- 放松监管：减少“安全设计”相关强制措施、放松人工智能监管，让企业有更多的自主权，释放创新活力。
- 重新聚焦短期网络威胁，减少对后量子密码学等前沿技术的长远部署，转而专注于目前的实际网络威胁。
- 减少国际合作力度，采取更为独立的国家安全策略。



特朗普再次当选后，可能会重新审视拜登政府在网络安全领域的政策和行政命令，鉴于二位在网络安全、经济、国际关系等关键政策上的理念差异，有理由推测特朗普可能会对拜登的网络安全行政令做出调整或重新定义。

1、总体政策方向：全面防护 vs. 重点防御

拜登政府的网络安全政策以广泛覆盖为主，致力于巩固美国的网络安全基础，涉及零信任架构、供应链安全、后量子密码学、人工智能和身份管理等多个领域。

2021 年拜登发布的网络安全行政令（EO 14028）推动部署多种安全措施，尤其是在联邦政府和关键基础设施中的防护措施。

相比之下，特朗普在其首个任期内（EO 13800）则更注重保护联邦网络和关键基础设施的网络安全，但整体策略更加聚焦于具体威胁，特别是防范国家级对手的网络攻击。政策上侧重于快速行动和减少监管，以提高政府机构和企业的灵活性和应变能力。

安全人士分析，如果特朗普在新任期内选择对拜登的网络安全行政令进行调整，他可能会减少对全面网络安全政策的关注，将更多资源集中于特定的国家安全威胁，并简化部分监管，以鼓励私营部门的快速响应。

特朗普时期设立的网络安全和基础设施安全局（CISA）在拜登政府时期不断发展壮大， 持续加强政府和关键基础设施的网络防护措施。在拜登政府的推动下，CISA 的预算从 2021 财年的约 20 亿美元扩大到 2025 年的 30 亿美元。2021 年，CISA 成立了联合网络防御协作组织，旨在改善网络安全公司、联邦政府和关键基础设施提供商共享信息的方式。

曾在特朗普上届政府的国土安全部任职的布莱恩 · 哈雷尔 (Brian Harrell) 表示，特朗普政府可能会为 CISA 提供资金，以开发更强大的威胁检测和响应威胁的能力，以及与各州和地方政府在网络安全方面进行更好的协调。

特朗普政府可能会为 CISA 提供资金，以开发更强大的威胁检测和响应威胁的能力，以及与各州和地方政府在网络安全方面进行更好的协调。

2、加大防御投入，推进网络现代化

尽管有业内人士预计，由埃隆 · 马斯克牵头、旨在削减 2 万亿美元联邦预算的计划可能会削弱美国的网络安全工作，但众多安全人士认为，为网络安全提供足够资金支持仍是特朗普政府的优先事项。布莱恩 · 哈雷尔表示，特朗普上任后不太可能立即开始削减网络和国家安全预算。一位业内高管甚至预测，特朗普政府将选择在网络领域投入更多资金。美国商会在选举前预测，无论哪位候选人获胜，将继续实施当前的网络安全政策。

实际上，网络安全是少数得到美国共和与民主两党共同支持的领域。国家网络安全联盟执行董事丽莎 · 普拉格米尔（Lisa Plaggemier）强调，网络安全是“特朗普政府和现任政府之间的两党议题，”“将网络安全建设作为优先事项的策略依然坚定、超越党派界限。”

一位接近过渡团队的人士表示，预计新一届特朗普政府将继续实施 2020 年未执行的网络政策。这意味着，要了解未来特朗普政府的网络安全政策，可以回顾一下他的首个任期。

2017 年，特朗普颁布行政令，强调 “关键基础设施保护”，呼吁联邦政府 IT 现代化”。次年，特朗普政府公布了该国 15 年来首个国家网络安全战略，放宽允许情报机构通过网络攻击“反击”对手的规则。同年，特朗普签署了《网络安全和基础设施安全局法案》，成立了同名机构，负责领导保护关键基础设施免受网络攻击的工作。

在网络威胁日益严重的时代，网络安全不仅是优先事项，而且势在必行。从交通运输到电网等关键基础设施暴露的漏洞越来越多，遭受的网络攻击也日益增多，网络威胁达到了前所未有的高度。网络安全基础设施需要进行前所未有的投资，也意味着未来的特朗普政府在网络防御将会强化其积极应对的策略。

在其首个任期，特朗普加快了信息保护法规的制定。其核心是网络安全成熟度模型认证（CMMC）计划规则。这项始于特朗普首个任期的标准，在拜登的任期内得以延续，并即将发布最终的计划规则。

共和党全国委员会 2024 年 7 月发布的《政策路线图》，将保护关键基础设施免受黑客攻击列为 “国家优先事项”，这是整个文件中唯一提到网络相关的内容。《政策路线图》承诺，将“提高关键系统和网络的安全标准”“动

用一切国家力量工具”来保护美国关键基础设施和国家工业基础“免受恶意网络攻击”。

特朗普政府承诺部署“所有工具”来保护重要资产，这表明其将继续致力于加强国家防御，优先防止国家级对手窃取政府、联邦承包商及其供应链所掌握的关键信息。这一做法可能意味着特朗普政府将加大对尖端网络防御的投资，同时与私营科技公司加强合作，打造坚固弹性的系统，以抵御未来的网络威胁，尤其是来自敌对国家的威胁。

“我们将以国家安全为重点，重点保护关键基础设施、政府网络和关键行业免受网络威胁。”在特朗普第一任期内担任网络安全和基础设施安全局基础设施安全助理主任的布莱恩·哈雷尔说。

3、放松监管，实现全面逆转

美国律师事务所 Hunton Andrews Kurth 的合伙人丽莎·索托 (Lisa Sotto) 认为，放松监管将成为特朗普政府的首要主题。哈雷尔也认为：“特朗普 2.0 时代的网络安全政策可能会侧重于消除多余的监管，增加安全能力，减轻来自中国、人工智能和量子计算的威胁。”

近四年来，拜登政府一直试图让美国科技公司和基础设施运营商对国家的网络安全态势承担更多责任，并限制间谍软件的传播，对人工智能设置护栏，并打击网上虚假信息。但当特朗普上任后，几乎肯定会取消或大幅缩减这些限制，转而支持有利于商业的网络战略，并强调对敌对国家的网络军队发动积极攻势。

因此，预计未来的特朗普政府可能会放弃拜登雄心勃勃的计划，即对目前缺乏安全保障的美国基础设施实施网络监管。这一努力在铁路、输油管道和航空领域取得了成果，但在水利和医疗卫生等领域却遭遇挫折。

尽管针对重要系统的网络攻击日益增多，共和党的政纲承诺“提高关键系统和网络的安全标准”，特朗普政府不太可能支持对基础设施运营商实施新的监管要求。

美国战略与国际研究中心高级副总裁兼战略技术项目主任詹姆斯·刘易斯认为，“（将来）未经国会明确授权，将不再进行监管”。哈雷尔则表示，拜登任期内充斥着新的网络监管，有时会让行业感到困惑和负担过重。“未来白宫将寻求简化合规流程，降低监管负担。”

但一位美国网络官员表示，这种做法可能不会持久。“最终特朗普政府会认识到，网络监管对于确保关键基础设施的安全是必要的。”民主防御基金会网络与技术创新中心高级主任马克·蒙哥马利（Mark Montgomery）则预测，为保护脆弱的行业，特朗普政府将在安

特朗普政府承诺部署“所有工具”来保护重要资产，这表明其将继续致力于加强国家防御，优先防止国家级对手窃取政府、联邦承包商及其供应链所掌握的关键信息。

全防护措施中强调合作和激励手段。

削减“安全设计”合规监管。拜登的网络安全政策强调，软件和设备制造商在产品安全性上承担更大责任，强调“安全设计”（Secure by Design）原则，即在产品设计阶段即嵌入安全防护，防范潜在的供应链漏洞。为此，拜登政府在联邦政府层面推进了多项强制性网络安全标准； CISA 则在过去几年发起一场宣传活动，鼓励企业“从设计上保证产品安全”，希望在企业中形成自上而下的安全责任文化，要求企业在防护设计、数据管理和威胁检测方面承担更多的合规责任。

民主党政府利用“安全设计”推动新的监管，但未来特朗普执政期间，安全设计最多可能是一个口号。”预计，特朗普可能会削减此类合规监管，不过多地推行“安全设计”原则，给予企业更多的自由，鼓励企业自行采取安全防护措施，以灵活、快速地应对安全威胁，而不是通过强制性标准实施。然而，鉴于供应链安全问题在过去几年屡次引发重大事件（如太阳风安全事件），特朗普或会在某些高风险领域保留拜登的供应链安全策略。

废除人工智能行政令。特朗普的竞选团队已经暗示，计划审查并可能废除拜登政府实施的有关人工智能发展指南的行政令。特朗普团队认为，放松监管限制可以释放创新活力——这对于在与中国日益激烈的人工智能竞赛中竞争至关重要。拜登任期内成立的人工智能安全研究所旨在平衡创新与严格的监管保障。特朗普的政策将强调人工智能的快速发展，同时探索在监管阻碍进展的领域放松管制。特朗普团队表示，加强国家的人工智能基础设施和营造有利于创新的环境对于国家安全和经济主导地位至关重要。

蒙哥马利也认为，
特朗普可能对国家网络防御“采取更积极的方式”，
包括让国民警卫队在保护国内基础设施方面
“发挥更重要的作用“。

4、比“前置防御”更加大胆的战略

特朗普从拜登政府手中接过接力棒的一个领域是政府使用军事手段对黑客攻击，以及对外国对手的网络行动作出反应。

在拜登的领导下，美国军方网络司令部扩大了与盟友在海外追捕黑客的行动。但共和党敦促拜登对国家级的黑客攻击活动做出更强硬的回应，特朗普很可能会采取这种做法——尤其是在他选择众议员迈克 · 沃尔兹（Mike Waltz）担任国家安全顾问之后，沃尔兹主张对攻击组织实施网络攻击。

蒙哥马利也认为，特朗普可能对国家网络防御“采取更积极的方式”，包括让国民警卫队在保护国内基础设施方面“发挥更重要的作用”。

蒙哥马利还预计，美军网络司令部将开展更频繁、更强有力的进攻行动。在其第一任期内，特朗普将网络司令部提升为完整的作战司令部。他预测，特朗普政府将“更赞成”成立单独的军事网络部门。

2024 年 9 月，奥本大学麦克拉里网络与关键基础设施研究所和网络空间日光浴室委员会 2.0 的 40 名网络安全专家发布了 39 项建议，为下一届政府提供了网络安全政策建议路线图。

专项工作组认为，现在是采取大胆、果断行动的时候。特别工作组特别强调，需要“超越纯粹的防御态势，让那些在网络空间对美国造成伤害的组织承担真正的代价”。 对此，Gartner 高级副总裁分析师卡黛儿 · 蒂勒曼表示，这一立场比国防部 2018 年为网络安全推出的“前置防御”战略更加大胆。

网络安全政策建议路线图建议新政府使用“所有国家力量——外交、经济，必要时还有军事”来应对网络攻击。地缘政治和技术顾问凯文 · 艾利森 (Kevin Allison) 表示：“特朗普政府在决定如何在网络空间反击对手时，将考虑全套

随着对监管的关注度逐渐降低，
特朗普的第二任期可能会继续打击网络攻击活动，
并采取更积极的方式来解决勒索软件问题，
包括更多地使用攻击反击手段。

政策手段。

5、减少国际合作，推行更独立的防御策略

拜登政府的网络安全政策更强调国际合作，与盟国在网络威胁和网络政策方面紧密协作。为此，拜登政府加强了与欧洲、亚太等地区的网络安全伙伴关系，以共同应对各种国家级网络攻击。

鉴于特朗普在外交政策上倾向于“美国优先”，未来的政府可能会减少在网络安全上的国际协作，更专注于独立的国家防御战略。特朗普倾向于通过对外施压来达成网络安全目标，而非通过跨国协作来推动整体安全框架的建立。然而，由于全球网络安全形势复杂，特朗普可能会在特定领域保持有限的国际协作。

此外，拜登政府提出加速向后量子密码学的迁移，旨在为可能出现的量子计算威胁做准备。拜登的网络安全行政令鼓励联邦政府和私营部门协作，提前应对量子技术对传统加密技术的潜在威胁。

特朗普政府在量子计算领域支持技术创新，但可能不会如拜登政府般密集推行后量子密码学的标准。特朗普的网络安全政策或许会更多地聚焦于短期威胁，可能放缓后量子密码学的推广步伐。

6、总结

随着对监管的关注度逐渐降低，特朗普的第二任期可能会继续打击网络攻击活动，并采取更积极的方式来解决勒索软件问题。 众包安全平台 Bugcrowd 创始人凯西 · 埃利斯 (Casey Ellis) 预计，美国的网络攻击能力将会增强，包括更多地使用攻击反击手段。

- 特朗普和拜登在总统任期颁布过的网络安全总统行政令，虽然在具体政策细节上有所不同，但都聚焦于提升联邦网络和关键基础设施的安全性。拜登的网络安全策略侧重于全面的系统防护，注重“安全设计”和供应链安全，而特朗普则更加偏向简化监管，灵活应对实际威胁。特朗普新政府可能会保留部分拜登的网络安全政策基石，同时进行调整以使政策更具灵活性，并减少对企业的监管，以符合其一贯的“减少政府干预”理念。
- 特朗普可能对拜登的网络安全监管政策进行部分削弱，但在面对国家级威胁和关键基础设施保护方面，特朗普或将延续强化防护措施，以维护美国的网络安全根基。此外，特朗普也会使用“所有国家力量——外交、经济，必要时还有军事，来应对网络攻击”。

巩固网络安全遗产：拜登的最后一项网安行政令

特朗普胜选后，业界普遍预测“跛脚鸭总统”拜登很可能在 2024 年年底前颁布第二项网络安全总统行政令，以在卸任前完成更多网络安全政策的布局。

据消息人士透露，这项总统令预计将在国会“跛鸭期”内发布，重点关注联邦网络标准和新兴技术威胁，覆盖从“安全设计”倡议到供应链责任、IT 和运营技术安全、互联网路由、密码管理、身份管理、人工智能，以及网络安全人才培养等一系列主题。

奥巴马时代国家安全委员会网络安全协调员、现任非营利性网络威胁联盟负责人的迈克尔·丹尼尔 (Michael Daniel) 表示，特朗普重新入主白宫，拜登政府公布行政措施是合乎逻辑的。

新的总统行政令重点包括如下内容。

1、通过行政令巩固网络安全政策

消息人士表示，拟议中的行政令将解决拜登政府 2021 年网络安全行政令未曾涉及或未完全涉及的领域。一位消息人士将这项新命令描述为一项“彻底的”法令，将解决美国网络安全政策领域中未完成的工作。

其中，推进向后量子密码的迁移，预计也将成为即将出台行政令的一个主要内容。这一标准旨在应对未来量子计算机可能突破传统加密的威胁，确保政府和企业网络环境的安全性。

即使在拜登任期的最后数月，白宫也在努力完成大量网络安全和技术政策议程。2024 年 10 月下旬，白宫与财政部发布了一项最终规则，禁止在人工智能、半导体和量子计算等先进技术领域开展对外投资，以保护美国的国家安全态势。

2024 年 10 月底，拜登政府宣布禁止在 AI、半导体、量子计算等高科技领域进行对外投资，以防关键技术

外流，削弱美国的技术主导地位，影响美国国家安全。

作为拜登政府 2024 财政年度结束前，在系统中实施零信任架构期限的一部分，整个联邦生态系统的各机构一直在加快其内部安全态势提升工作。

拜登政府意图通过该项行政令巩固其在科技和网络安全领域的遗产。迈克尔 · 丹尼尔（Michael Daniel）表示：“拜登政府在 12 月份颁布这一行政令是合理的选择。”丹尼尔认为，颁布这一行政令不仅是为应对特朗普上台后可能出现的政策调整，也为确保网络安全政策的连贯性打下基础。

2、聚焦政府身份管理，促进零信任架构迁移

据另一位熟悉行政令草案内容的人士称，预计该行政令将部分侧重解决政府部门的身份和访问管理，以确保在网络威胁日益复杂的环境下关键政府数据的安全，而非期待已久的覆盖每个美国人的数字身份行政令。

2024 年 3 月，白宫曾表示，在制定针对公共福利计划身份盗窃的行政令，以减少福利计划欺诈行为。根据该计划的草案，任何公共福利计划都必须向用户提供公共运营的数字身份服务，作为访问服务的一种方式。此前有报道称，在疫情期间启动或扩大的救济计划中存在大量身份盗窃行为。

在政府层面，联邦机构已在加速改进内部网络安全态势，以在 2024 财年结束前，实现零信任架构的全面实施。

2022 年 1 月 26 日，拜登总统办公室向联邦政府行政部门和机构负责人发布了一份行政备忘录，为零信任架构 (ZTA) 战略提供指导和方向。备忘录“提出了一项联邦零信任架构 (ZTA) 战略，要求各机构在 2024 财年结束前达到特定的网络安全标准和目标，以加强政府对日益复杂和持续的威胁活动的防御能力。”

在政府层面，
联邦机构已在加速改进内部网络安全态势，
以在 2024 财年结束前
实现零信任架构的全面实施。

根据白宫管理和预算办公室（OMB）的备忘录，各机构必须在 2024 年 9 月 30 日之前放弃基于边界的防御。因此相关机构必须在 2024 年 11 月提交更新的零信任架构实施计划，概述将如何实现关键的安全目标，包括消除隐性信任、保护关键资产及持续实时验证用户和设备。

CISA 零信任计划负责人布兰迪 · 桑切斯 (Brandy Sanchez) 表示，“随着各机构准备提交更新的零信任实施计划，网络安全和基础设施安全局正在与 OMB 和利益相关者进行协调，以确保对即将发布的定性数据进行彻底审查。”

桑切斯表示，“CISA 和 OMB 将加强对整个联邦政府采用零信任的技术援助。”CISA 还将评估各机构如何“测试其零信任框架的有效性”，例如，在模拟攻击场景中使用渗透测试和 MITRE ATT&CK 评估，以衡量对已知网络攻击技术的防御能力。

2024 年 6 月，美国国防部首席信息官发布了一份近 400 页的“零信任覆盖”文件，旨在作为路线图和指南，帮助该部门实现拜登政府行政令中提出的目标。零信任尚未在国防部整个部门实施，但到 2027 财年，预计将达到“目标水平”实施。这意味着美国国防部已实施了其《零信任战略和路线图》中确定的 152 项目标中的 91 项。

联邦首席信息官克莱尔 · 马托拉纳 (Clare Martorana) 在 2024 年 9 月表示，一些主要联邦机构在 9 月 30 日的最后期限前已在其网络上建立并采用一定程度的零信任架构。24 个联

邦监管机构“全部处于 90% 的高位”。但她早些时候曾承认，对于零信任的持续推进和确保各机构能在预算优先事项和资源不断变化的情况下有力推进零信任架构而言，持续的资金投入是一项关键挑战。

> “安全设计”的思维转变可能需要较长时间才能扎根，就像汽车安全带和安全气囊花了几十年才被广泛接受一样。

3、推进“安全设计”，鼓励内置安全

此外，这项行政命令还将涉及“安全设计”的原则。CISA 一直在推动安全的产品设计，鼓励企业在产品设计初期内置安全特性，以应对近年来多起高调的网络安全事件。

2023 年 3 月，拜登政府设立的网络安全办公室（ONCD）在发布了一项全面的政府网络安全战略，以推行安全设计原则，敦促开发人员采用内置防护功能的内存安全编程语言，以防止黑客造成的未经授权的访问、数据破坏或系统崩溃。白宫网络办公室还在努力提高边界网关协议（BGP，一种骨干数据传输算法）的安全性。

美国网络安全和基础设施安全局 (CISA) 局长珍 · 伊斯特利 (Jen Easterly) 表示，在推进“安全设计”计划时，CISA 是基于对长期趋势的认识。她表示，“在过去四十年中，从互联网的诞生到软件的大规模采用，我们见证了一场技术革命，迫使安全和保障退居次要地位，技术制造商和软件生产商优先考虑上市速度和功能，而不是安全性。”

自 CISA 于 2023 年启动“安全设计”倡议以来，已有近 170 个机构签署了承诺。据悉，签署承诺者将会采取一系列措施来减少产品的漏洞，包括建立默认的多因素身份验证和其他形式的防网络钓鱼身份验证保护，并减少使用默认或硬编码密码。这些企业还承诺通过官方渠道更加透明地披露安全漏洞，做出专门努力减少常见漏洞，并帮助客户快速安装安全补丁。

但她指出，这种“安全设计”的思维转变可能需要较长时间才能扎根，就像汽车安全带和安全气囊花了几十年才被广泛接受一样。

4、为下一阶段的网络安全工作奠基

丹尼尔指出，新的网络安全行政令不仅是在收尾现有政策，更是为未来进一步强化网络安全奠定基础。“从整体上看，美国的网络安全防护已得到提升，但离理想状态还有距离。”

特朗普的当选为拜登政府推进这一政策增添了紧迫性。拜登第二道总统行政令的核心目的是确保拜登的网络安全遗产得以延续，也为下届政府预留了继续推进网络安全政策的空间。

分析：特朗普网安政策影响与应对

2024 年美国大选，特朗普最终获得 312 张选举人票，取得压倒性胜利。共和党也同时拿下参众两院，这意味着特朗普将拥有超级执政权力，推行他的激进主张。

尽管特朗普与哈里斯之间的选举竞争，更多围绕生育权、移民、经济等国内政策。两者都未提出处理关键网络问题的政策与计划，但从相关分析与报道中，两者在网络安全政策差异及潜在影响仍可看出端倪。

分析显示，与代表民主党的哈里斯相比，特朗普将在网络安全方面更加激进，包括对我国采取更主动的攻击行动、鼓励人工智能领域的竞赛，以及加大针对我国的信息战投入等方面。

一、网安问题超越两党界限，对华强硬是主流

分析人士认为，网络安全是美国民主、共和两党共同关心的问题，其背后的驱动因素来自国家威胁而非社会或经济问题。通常的党派界限在这里并不总是适用。这意味着无论特朗普还是哈里斯谁能胜出，在利用网络安全话题攻击和妖魔化中国方面，两党将会有着共同的诉求和主张。

拜登政府的相关网络政策足以说明这一点。拜登政府保留了特朗普第一个任期内的很多国家安全和网络安全政策。例如，特朗普政府期间成立的美国网络安全和基础设施安全局（CISA）；以及特朗普任期内启动的“总统杯网络安全大赛”等大型联邦活动。第六届年度总统杯网络安全竞赛将于 2024 年 12 月启动。

近年来，美国持续以网络安全问题对中国进行打压。美国相关智库机构甚至指责，中国成为美国的主要网络威胁，称“中国已经做好准备并计划通过制造混乱和不和来破坏美国社会”。

2023 年 5 月，“五眼联盟”国家（美国、英国、加拿大、澳大利亚、新西兰）的网络安全主管部门联合发布预警通报称，名为“伏特台风”的中国黑客组织，针对美国关键基础设施单位实施了网络间谍活动。2024 年 1 月，美国联邦调查局局长克里斯托弗·雷向众议院中国竞争特别委员会表示，与中国政府有关的黑客正瞄准美国关键基础设施，准备对美国人造

分析人士认为，网络安全是美国民主、共和两党共同关心的问题。
在利用网络攻击攻击和妖魔化中国方面，两党将会有着共同的诉求和主张。

成“现实世界的伤害”。他称，美国水处理厂、电网、石油和天然气管道及交通枢纽，都是中国国家支持的黑客行动的目标。

在网空领域，利用网络攻击事件对华施压已成为两党共识，特朗普将会持续利用这一问题对华施压。

二、未来特朗普政府对华网络攻击将会更主动

目前，特朗普这位共和党总统候选人，尚未提出处理关键网络问题的详细政策与计划。今年早些时候，美国传统基金会发布的《2025 项目》报告，被视为特朗普第二届政府的政策蓝图，其中，提出大幅削弱网络安全和基础设施安全局 (CISA) 职能及其他网络安全政策的构想，可能未必全部实施。但相关人士仍然可以从中拼凑出特朗普第二任期的网络安全政策方向。

1、鼓励军方实施“进攻”，而不是专注于阻止网络威胁。

据媒体对五位前特朗普政府高级官员的采访，大多数受访者认为，特朗普政府的国家安全方针将会比现任政府更强硬、行动更快。他们都表示，特朗普本人在网络安全政策上投入了大量心思和时间。

在特朗普第一个任期内，美国政府将网络威慑作为其网络安全战略的核心支柱，提出了以“前置防御”和“持续交手”为核心的进攻性威慑策略，对外开展低烈度的网络攻击。

预计，美国讨论已久的网络部队将会组建，以进一步提升所谓的网络进攻能力。此外，美国可能还会以互惠对等为由，限制中国等国对美国互联网和关键基础设施对访问；同时持续推动对 TikTok 等中国互联网应用等监管限制与打击。

2、进攻网络行动重点转移到中国和伊朗。

据受采访的前政府官员透露，特朗普可能会将进攻性网络安全工作重点从俄罗斯和朝鲜转移到中国和伊朗。据路透社发布的消息，在特朗普第一个任期内，就授权中央情报局对发动攻击性网络行动：即在中国社交媒体实施秘密活动，引导中国公众舆论反对中国政府。三名前官员透露，中情局为此组建了小型特工团队，使用虚假网络身份传播中国政府的负面言论，同时向海外新闻媒体泄露诋毁性情报。这一行动始于 2019 年，此前从未被报道过。

3、放松监管增加投入，加码中美人工智能竞赛。

特朗普本人关注人工智能的应用，重视确保美国在中国和其他对手的竞争中保持领先地位。因此预计，特朗普将支持放松对人工智能和其他新兴技术的监管，制定更有利于商业的网络安全政策。

前 CISA 助理部长哈雷尔（Brian Harrell）表示：“特朗普第二任期的网络安全政策可能会侧重于消除多余的监管。此外，特朗普政府可能会再次增加人工智能和量子信息科学等科

技的经费；在人工智能芯片等技术出口限制上持续加码，同时推动联邦机构的人工智能部署和采用。作为在人工智能、量子等领域与中国竞争的重要措施。

4、加强关基设施安全监管，多手段保护美国利益。

针对未来新政府可能加强网络防护的举措，前任网安官员预计，（特朗普政府）将可能会提高关键基础设施提供商和业主的标准，为 CISA 提供资金，以开发更强大的威胁检测和响应能力，加强与州和地方政府的协调，加大对保护工业控制系统 (ICS) 举措的支持。

保守派智库 R 街研究所 (R Street Institute) 网络和新兴威胁团队政策主管布兰登 · 普格 (Brandon Pugh) 也认为，尽管共和党政府不愿实施严格的监管，但特朗普仍有可能以国家安全的名义对关键部门实施基本的网络要求。

此外，未来特朗普政府将会采取从网络攻击、制裁到外交等多个层面的手段，加强对关基设施的防护。 前能源部前高级网络官员肖恩 · 普兰基 (Sean Plankey) 表示：“我们会从战略和战术角度利用网络空间行动，来实现美国的国家安全目标。”

三、美网络安全政策影响与应对建议

根据初步披露的提名信息，特朗普政府的组成由多个对华强硬的人士组成，除了在贸易政策上对我国施压，一定会利用其网络安全政策对我进行打压。

建议研究可能的风险与问题，从多个角度进行防范：

1、持续增加我国应对网络攻击，尤其是国家级网络攻击的能力。

正如美国的网络攻击与防护，充分发挥了公私机构和民间人士的作用，我国也应该建立起公私能力协作、信息共享的常态化机制，确保我国保持应对美西方的进攻性网络攻击的能力。

2、充分利用人工智能技术，加强对社交媒体的监测，消除内容风险。

美西方的信息战会充分利用各国的社交媒体，发布虚假的信息，抹黑丑化我国政府与领导人，放大社会事件的负面影响，我国应尽快依靠先进的人工智能技术，建立识别发现和快速阻止此类信息传播的能力 。

3、为中美博弈中的科技企业提供必要法律与资金支持。

为实现打压和阻碍中国科技发展的目标，美西方会利用政策和技术等多种手段，对我国人工智能、网络安全及社会化媒体等科技企业实施打压和封锁，需要我国政府部门成立专门组织因应，提供包括政策、法律和资金方面的支持。

4、将推动网络安全能力与体系现代化落到实处。

目前美国、欧盟都在推动旨在提升网络防护能力的现代化，尤其是明确要求政府机构和关基部门采用零信任、供应链等先进技术，且规定了达标时间。我国主管部门也在推动安全能力与体系现代化，但在推进方面相对笼统，缺乏可实施、具有约束力的要求，建议网安全主管部门针对美国的措施，制定出技术要求明确、效果可验证的实施计划。

> 建议网安全主管部门针对美国政府的网络现代化措施，制定出技术要求明确、效果可验证的实施计划。

CTFWAR.ORG

网络安全的本质是攻防对抗
讲百遍不如打一遍

---习近平

CTFWAR介绍

CTFWAR攻防战争平台是CTFWAR网络安全攻防对抗联赛的官方平台，是由中国网络安全攻防大咖联合发起的创新型学习平台，以游戏的形式融入多种网络攻防场景进行答题、竞赛、互动。CTFWAR攻防靶场分为初级新手区、中级进阶区、高级挑战区，同学们可根据自身技术能力及技术方向进行筛选，整个学习过程将有全面的数据化呈现。

攻防答题模式

CTFWAR攻防战争平台采取主流的CTF夺旗赛和AWD攻防赛的答题模式，提供云端的攻击终端，同学们在云端攻击平台上进行攻防实战操作，通过 Flag 判定和操作用时进行综合评分，以获得积分升级和金币奖励。

积分等级体系

CTFWAR攻防战争平台采取主流的CTF夺旗赛和AWD攻防赛的答题模式，提供云端的攻击终端，同学们在云端攻击平台上进行攻防实战操作，通过 Flag 判定和操作用时进行综合评分，以获得积分升级和金币奖励。

中外安全事件处罚对比：重锤还是搔痒，网安事件应罚多少?

罚款，是世界各国对系统运营者网络安全违法责任的明确标价。只不过标价的方式和价位有所不同，对运营者的“震慑”程度也有所不同。相比于某些国家动辄数百万，上亿元的“重锤式”罚款，中国监管机构仅给出10万元以下的罚款，可以用“挠痒痒”来形容了。

各国的国情不同，监管目标也不同，我们不能用简单的、一刀切的判断方式判断谁对谁错。但是，一个显而易见的事实是，当罚款金额显著高于建设成本时，运营者就会自然而然的选择投入资金进行必要的网络安全建设；反之，如果罚款金额远远小于建设成本，那么，在自身尚未产生明确的经济损失之前，运营者也会自然而然的选择“碰碰运气”，放弃网络安全建设与投入。

笔者就曾经历过这样一件事：有一所高校，因为发生重大数据泄露事件，被判罚 80 万元。于是这家高校就向很多安全公司咨询了数据安全的建设方案。结果发现，就这所高校的实际情况而言，各家安全公司给出的最低报价都是接近于 200 万元。最后这家高校咬了咬牙，还是放弃了数据安全建设项目。毕竟，建设了就是要投入 200 万，不建设也未必一定会被处罚，而且一次性建设投入，足够被罚两次半了。

本文将为大家总结一下 2024 年以来，媒体公开报道的国内外网络安全处罚事件，并对国内外的罚款金额进行对比分析。如果某些处罚案件的公开信息中，没有明确具体的处罚金额，本文将不进行收录和分析。

> 一个显而易见的事实是，
> 当罚款金额显著高于建设成本时，
> 运营者就会自然而然的选择投入资金
> 进行必要的网络安全建设。

1、2024 年国内网络安全处罚事件与罚金分析

下表给出了 2024 年媒体报道的10件国内机构网络安全责任处罚事件，部分处罚事件实际发生在 2023 年，但直到 2024 年才被集中报道出来。其中，涉及数据泄露的处罚事件 7 件，

时间	被罚机构	处罚机构	主要处罚原因	罚金（RMB）
2023.6	某生物技术公司	公安	19.1GB 个人信息泄露	5 万元
2023.7	某教育公司	公安	12 万 + 条个人信息泄露	5 万元
2023.8	某教育公司	公安	70 多万订单信息泄露	5 万元
2024.1	某科技公司	网信办	大量个人信息泄露	10 万元
2024.2	某超市	网信办	多台服务器、终端被木马控制	5 万元
2024.5	某集团	网信办	服务器被入侵，大量数据泄露	10 万元
2024.7	某培训学校	网信办	网页被篡改加挂涉黄违法链接	1 万元
2024.10	某 IT 公司	网信办	未落实等保，存在大量漏洞	5 万元
2024.10	某科技公司	网信办	大量敏感数据泄露	2 万元
2024.10	某两家公司	网信办	大量敏感数据泄露	10 万元

系统遭入侵 / 篡改等处罚事件 2 件，未履行网络安全义务处罚事件 1 件。总体而言，数据泄露事件，是国内机构被处罚的主要原因。

从处罚金额来看，绝大多数事件都是 5 万元或 10 万元。下面就对这些事件进行简要的介绍。

（1）泄露 19.1GB 数据，北京一生物技术公司被罚 5 万元

安全内参 2024 年 1 月消息，昌平网安部门在 2023 年 6 月的一次检查中发现，昌平某生物技术有限公司存在数据泄露的情况：其委托的另一软件公司研发的“基因外显子数据分析系统”中，包含大量公民个人信息、技术机密信息等需要加密保护的数据，但该软件公司在开发系统互联网测试阶段，未对相关数据进行加密，未落实安全保护措施，导致 19.1GB 的敏感数据被泄露。北京市公安局昌平分局依据《中华人民共和国数据安全法》（以下简称《数据安全法》）相关规定，给予该公司警告并处罚款 5 万元的行政处罚。

（2）泄露 12 万 + 条个人信息，北京某教育公司被罚 5 万元

安全内参 2024 年 1 月消息，北京朝阳网安部门 2023 年 7 月检查发现，朝阳某教育公司数据被泄露到境外非法网站上，该公司的一个客户关系管理系统内存储的该公司员工账号及对应客户姓名、手机、下单时间、成交金额等 12 余万条信息被泄露。造成这一泄露事件的原因是，该公司技术人员在对系统测试过程中，将有权限的测试账号设为弱口令，且系统正式使用后未将测试账号进行清空删除处理，进而导致系统被黑客入侵。北京市公安局朝阳分局依据《数据安全法》相关规定，给予该公司罚款 5 万元的行政处罚。

（3）泄露 70 多万订单信息，北京某教育公司被罚 5 万元

安全内参 2024 年 1 月消息，某境外黑产论坛于 2023 年 8 月，发布题为“某教育站点教 70 多万订单信息”的帖文。针对此情况，海淀网安部门立即开展核查处置工作。经查，该公司教务排课系统在账号密码传输前未进行加密，存在账号密码被爆破的可能。黑客可通过爆破手段获取账号密码，通过访问导出大批量后台数据，造成数据泄露。北京市公安局海淀分局《数据安全法》相关规定，给予该公司罚款 5 万元的行政处罚，给予直接负责的主管人员罚款 1 万元的行政处罚。

总体而言，依照目前的国内相关法律法规对政企机构做出的行政处罚，尚无法对涉事机构起到震慑作用，涉事机构的违法成本相对较低。

（4）泄露个人信息，北京某科技公司被罚 10 万元

2024 年 1 月，衡阳市网信办检查发现，某个在衡阳从事做软件开发业务的北京科技公司，其开发应用的网站数据库存在未授权访问漏洞，造成了公民个人信息泄露。经查，该科技公司主要为教育类单位提供互联网软件应用与开发服务。2023 年 1 月，该公司开发了一家网站用于教学，同时也存储了包含用户姓名、手机号、电子邮箱在内的大量个人信息。但由于该公司在开展数据处理活动时并未加强风险监测，系统存在安全漏洞，造成个人信息泄露等问题。衡阳市网信办依据《 数据安全法 》相关规定，给予该公司罚款 10 万元的行政处罚。

（5）计算机遭黑客远程控制，南昌一超市被罚 5 万元

2024 年 2 月，南昌市网信办在日常的网络安全监测中发现，属地某连锁超市所属 IP 疑似被黑客远控，频繁对外发起网络爆破攻击。经调查发现：该连锁超市未对运营的网络及信息系统开展网络安全等级保护测评等相关工作，所属的服务器和多台终端感染木马病毒，且未能及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险，导致被控终端与服务器持续对内、对外发起大规模网络攻击，严重危害网络安全。南昌市网信办依据《 中华人民共和国网络安全法 》（以下简称《 网络安全法 》）相关规定，给予该连锁超市罚款 5 万元的行政处罚，给予直接负责的主管人员罚款 1 万元的行政处罚。

（6）大量数据遭境外窃取，南昌某公司被罚 10 万元

2024 年 5 月，南昌市网信办在日常的网络安全监测中发现，南昌某集团有限公司所属 IP 疑似被黑客远程控制，频繁与境外通联，向境外传输大量数据。经调查发现：该公司未采取相应的技术措施和其他必要措施保障数据安全，所属的服务器遭境外黑客攻击并植入可获取服务器文件管理权限和命令执行权限的木马程序，大量数据疑似遭泄露或被窃取。南昌市网信办依据《 数据安全法 》相关规定，给予该公司罚款 10 万元的行政处罚，基于直接负责的主管人员罚款 2 万元的行政处罚。

（7）网站被篡改，长沙一培训学校被罚 1 万元

2024 年 7 月，长沙市望城区网信办调查发现，长沙某职业技术培训学校所属多个网站多次被不法分子篡改加挂涉黄违法有害链接信息，在多次收到网信部门下达的整改通知后，仍未按照网络安全等级保护制度的要求，履行网络安全保护义务。长沙市望城区网信办根据《 网络安全法 》相关规定，

给予该培训学校罚款 1 万元人民币的行政处罚。

（8）存在安全漏洞，湖南一 IT 公司被罚款 5 万元

2024 年 10 月，湖南省互联网信息办公室在工作中发现，湖南某信息技术有限公司未落实网络安全等级保护制度，未采取相应的技术措施和其他必要措施保障数据安全，系统存在未授权访问漏洞，网络安全日志大量缺失，严重损害数据安全。湖南省互联网信息办公室依据《数据安全法》和《湖南省网络安全和信息化条例》相关规定，给予该公司警告并责令改正，作出罚款 5 万元的行政处罚，并对该公司主管人员和直接责任人员作出罚款、2 万元和 1 万元的行政处罚。

（9）大量数据泄露，四川一科技公司负责人被罚 2 万元

2024 年 10 月，南充市互联网信息办公室在检查中发现，高坪区轩某科技有限公司自营业以来，相关责任人网络安全、数据安全意识淡薄，未建立网络安全、数据安全相关管理制度，数据安全保障技术手段不足，未履行网络安全防护和数据安全保护义务，并导致数据泄露。南充市互联网信息办公室依据《网络安全法》《数据安全法》相关规定，给予该公司责令改正，并对该公司负责人处以罚款 2 万元的行政处罚。

（10）大量敏感数据被窃取，河南两公司被罚 10 万元

2024 年 10 月，郑州市网信办在工作中发现，郑州市两家公司未履行网络安全保护义务，未采取必要的安全防护，导致大量敏感数据被窃取。郑州市网信办依据《数据安全法》相关规定，作出责令改正，给予警告并分别处以罚款 5 万元人民币的行政处罚。

经调查核实，郑州市某互联网信息服务有限公司在数据库中配置增加了远程登录空口令账户，导致黑客利用该空口令账户成功登录数据库，并窃取了数据库中的数据，被窃取的数据包括姓名、身份证号、手机号、邮箱地址等敏感信息。

另一起案件也非常相似。郑州市某科技有限公司缺乏网络安全意识，没有正确配置数据库，导致数据库存在未授权访问漏洞。攻击者通过漏洞登录数据库，查看、下载数据，导致敏感数据泄露。该公司系统访问日志功能未开启、重要的通联日志留存不足六个月，数据库系统配置不当，存在未授权访问漏洞。

小结

总体来看，国内的网络安全事件处罚主要呈现以下几个特点：

1、 事后处罚。绝大多数处罚事件都是在实际损失已经发生后，在检查相关企业时发现存在安全问题，再进行相应的处罚。

2、 处罚金额普遍较低，一般在 10 万元以下，甚至是 5 万元以下。

3、 部分处罚会涉及主要责任人，但处罚金额一般也不会超过 2 万元。

总体而言，依照目前的国内相关法律法规对政企机构作出的行政处罚，尚无法对涉事机构起到震慑作用，涉事机构的违法成本相对较低。

2、2024 年国外网络安全处罚事件与罚金分析

下表给出了 2024 年媒体报道的 18 件国外主管机构网络安全责任处罚。其中，涉及数据泄露的处罚事件 10 件，涉及违规跨境数据传输的处罚事件 2 件，违规分享数据处罚事件 4 件，其他原因遭处罚的事件 2 件。

从处罚金额来看，仅就本文收录的处罚事件而言，国外的机构受到的罚款，动辄数百万，甚至上亿美元，最少的一个处罚也有 99 万美元，约合人民币 715.5 万元。

从处罚金额来看，仅就本文收录的处罚事件而言，国外的机构受到的罚款，动辄数百万，甚至上亿美元，最少的一个处罚也有 99 万美元，约合人民币 715.5 万元。

时间	被罚机构	处罚机构	主要处罚原因	罚金
2024.7	阿里巴巴（电子商务）	韩国个人信息保护委员会	违规跨境传输个人信息	20 亿韩元
2024.4	Verizon（运营商）	美国联邦通信委员会	未经同意向其他机构分享用户数据	4690 万美元
2024.4	AT&T（运营商）	美国联邦通信委员会	未经同意向其他机构分享用户数据	5730 万美元
2024.4	T-Mobile（运营商）	美国联邦通信委员会	未经同意向其他机构分享用户数据	8010 万美元
2024.4	Sprint（运营商）	美国联邦通信委员会	未经同意向其他机构分享用户数据	1220 万美元
2024.5	Kakao（即时通信）	韩国个人信息保护委员会	泄露超 6 万用户个人信息	151 亿韩元
2024.5	必胜客（餐饮业）	澳大利亚通信与媒体管理局	违法发送垃圾邮件广告	250 万澳元
2024.6	Guidehouse（咨询公司）	美国司法部	APP 未经充分安全测试即上线，泄露大量个人信息	760 万美元
2024.6	NMA（咨询公司）	美国司法部	APP 未经充分安全测试即上线，泄露大量个人信息	370 万美元
2024.8	T-Mobile（运营商）	美国外国投资委员会	未能防止和报告敏感数据泄露事件	6000 万美元
2024.8	Uber（交通出行）	荷兰数据保护局	违反 GDPR 进行跨境数据传输	2.9 亿欧元
2024.9	AT&T（运营商）	美国联邦通信委员会	泄露超过 890 万名移动客户数据	1300 万美元
2024.9	Meta 公司（Facebook 母公司）	爱尔兰数据保护委员会	以明文形式存储数亿用户密码，并允许内部员工广泛访问这些密码	1.01 亿美元
2024.10	万豪（连锁酒店）	49 个州总检察长组成的联盟、美国联邦贸易委员会	泄露全球 3.44 亿用户个人信息	5200 万美元
2024.10	Check Point（网络安全）	美国证券交易委员会	在数据泄露事件中做出误导性披露	99.5 万美元
2024.10	Mimecast（网络安全）	美国证券交易委员会	在数据泄露事件中做出误导性披露	99 万美元
2024.10	Unisys（IT 集成商）	美国证券交易委员会	在数据泄露事件中做出误导性披露	400 万美元
2024.10	Avaya（通信服务商）	美国证券交易委员会	在数据泄露事件中做出误导性披露	100 万美元

罚款，动辄数百万，甚至上亿美元元，最少的一个处罚也有 99 万美元，约合人民币 715.5 万元。不得不承认，这是重拳出击。下面就对这些事件进行简要的介绍。

（1）未经同意，分享用户数据，美国四大运营商被罚近 2 亿美元

2024 年 4 月，美国联邦通信委员会（Federal Communications Commission，FCC）宣布，经过调查发现，电信运营商 Verizon、AT&T、T-Mobile 和 Sprint 在未经用户同意的情况下，将用户位置数据访问权限出售给数据聚合商，后者又将数据转售给第三方，并且这四家运营商即使在得知数据未经授权就被访问后仍继续出售给数据聚合商，并未采取任何措施确保第三方在被允许访问前取得用户同意。

FCC 表示，除非运营商获得用户的明确同意，否则必须对用户数据保密，因此决定对这四家运营商处以近 2 亿美元罚款。其中，Verizon 被罚款 4690 万美元，AT&T 被罚款 5730 万美元，T-Mobile 被罚款 8010 万美元，

Sprint 被罚款 1220 万美元（Sprint 和 T-Mobile 于 2020 年合并）。

（2）内部 VPN 遭漏洞攻击未向监管报告，这家金融巨头被罚超 7000 万元

2024 年 5 月，美国洲际交易所（ICE）因未能确保其子公司及时报告 2021 年 4 月出现的 VPN 安全漏洞，遭美国证券交易委员会（SEC）指控，需支付 1000 万美元罚款。

洲际交易所是一家位列《财富》500 强榜单的美国公司，在全球范围内拥有并经营多家金融交易所和结算所，包括纽约证券交易所。2023 年，该公司雇佣了超过 1.3 万名员工，报告总收入为 99.03 亿美元。

SEC 的调查显示：2021 年 4 月，有国家级攻击者，利用一个 VPN 安全漏洞，在一台 VPN 设备上安装了 Webshell 代码，试图窃取该设备处理的信息，包括员工姓名、密码和多因素认证代码。利用这些数据，威胁行为者或能访问内部企业网络。

美国《监管系统合规性和完整性》（Regulation SCI）法规要求，如公司发现入侵等安全事件，必须立即通知 SEC，并在 24 小时内提供更新，除非他们确定事件对其业务或市场参与者的影响微乎其微。而洲际交易所却足足花了四天时间评估事件影响，因此被判定违规。

（3）泄露超 6 万用户个人信息，韩国即时通讯巨头被罚 151 亿韩元

2024 年 5 月，因通信服务公司 Kakao 泄露超 6 万用户的个人信息，韩国个人信息保护委员会（PIPC）在全体会议上批准了对该公司 151 亿韩元的罚款，约合 7822 万元人民币。

此前有报道称 KakaoTalk 开放式聊天用户的个人信息被非法交易。一个交易在线营销计划的网站上出现了提供提取开放式聊天室参与者真实姓名和电话号码的广告。2023 年 3 月，PIPC 对此展开调查。

PIPC 调查发现，黑客在开放的聊天室中找到用户的临时用户名，然后使用 KakaoTalk 的“添加好友”功能和非法黑客程序，获取用户的会员序列号及其他信息。这些数据被组合起来创建个人信息文件，然后在 Telegram 等平台上出售。一位 PIPC 官员表示，“我们确认 696 名开放聊天室用户的信息被发布在特定网站上，而黑客访问了至少 65719 条个人信息记录。”

PIPC 得出的结论是，Kakao 没有对开放式聊天服务参与者的临时 ID 进行加密，因此很容易识别会员序列号，而临时 ID 中包含常规聊天会员序列号，被指出是数据泄露的重要原因。

（4）违规发送垃圾邮件，必胜客被罚 250 万澳元

2024 年 5 月，澳大利亚通信与媒体管理局（Australian Communications and Media Authority，ACMA）宣布，在接到消费者投诉后，判定 Pizza Pan Group Pty Ltd（必胜客）违反《2003 年垃圾邮件法》（Spam Act 2003，以下简称《垃圾邮件法》），向未经同意或已取消订阅的顾客发送 590 万条营销信息。被判处 250 万澳元（约合 167 万美元）的罚款。

ACMA 表示，其收到投诉，称连锁餐厅必胜客向已撤回接收营销信息同意的消费者发送营销信息。此外，投诉人称这些信息没有有效的取消订阅功能。

（5）上线前未做安全测试，美国两家知名企业被罚 1130 万美元

2024 年 06 月，美国知名咨询公司 Guidehouse 和 Nan McKay and Associates（NMA）在新冠（COVID-19）援助部署过程中存在

2024 年 08 月，GDPR 罚款“单王”诞生。荷兰数据保护局（DPA）对全球出行巨头优步（Uber）开出了一张创纪录的罚单，罚款金额高达 2.9 亿欧元（约合 3.24 亿美元）。

网络安全缺陷，被控违规。这两家公司已同意支付总计 1130 万美元的罚款。

具体来说，Guidehouse（前身为普华永道美国公共部门，总部位于弗吉尼亚州麦克莱恩）支付 760 万美元，NMA（总部位于加利福尼亚州埃尔卡洪）支付 370 万美元。根据和解协议，揭发此事的前 Guidehouse 员工将获得 194.925 万美元（约合 1414 万元人民币）的奖励。对于去年收入高达 55 亿美元的 Guidehouse 来说，这笔罚金微不足道。相比之下，NMA 的年收入大约为 1.9 亿美元。

美国司法部上月发布的和解协议披露了事件详情。两家公司被纽约州选中管理该州的紧急租赁援助计划（ERAP）。ERAP 由美国国会在 2021 年年初建立，覆盖美国全境，是联邦政府新冠疫情救济资金计划的一部分。在疫情封锁期间，这些安全网计划为低收入人群提供财政援助，帮助他们支付租金、水电费和其他与住房相关的费用。

在纽约州，临时和残障援助办公室负责该任务，并在 2021 年 5 月与 Guidehouse 签订了一份 3.1 亿美元的合同，指定其为主要承包商，负责向纽约居民提供 ERAP 技术和服务。NMA 作为 Guidehouse 的分包商，负责向纽约州居民提供提交租赁援助在线申请的 ERAP 系统。

两家咨询公司本应确保该 ERAP 应用程序在部署前经过适当的网络安全测试。但根据和解协议，NMA 和 Guidehouse 在测试工具未能发挥作用的情况下，依然批准应用程序上线。自 2021 年 6 月 1 日上线后，个人敏感信息的泄露几乎立即开始。在 ERAP 应用程序上线约 12 小时后，临时和残障援助办公室通知两家咨询公司，申请者的某些数据已经泄露到互联网上。

（6）违规跨境传输用户信息，阿里被罚约 20 亿韩元

2024 年 7 月，韩国个人信息保护委员会（以下简称“PIPC”）在第 13 次全体会议上，决定对违反个人信息保护法规跨境传输用户个人信息的 Alibaba.com Singapore E-Commerce Private Limited（以下简称“阿里”）处以 19 亿 7800 万韩元（约合 1025 万元人民币）的罚款和 780 万韩元（约合 4 万元人民币）的滞纳金，以及责令整改并提出改进建议。

PIPC 指出，当用户在阿里的某个平台上购买商品时，卖家会配送商品，并在此过程中将消费者的个人信息跨境传输给发货工厂，经查实，已有超过 18 万韩国用户的个人信息被提供给了中国卖家。

以该种方式跨境传输个人信息。很难根据法律规定的采取适当保护措施。韩国《个人信息保护法》要求企业必须在信息主体明确知晓的情况下获得其同意，并在与用户的合同内容中反映安全性保障措施、个人信息侵犯的投诉处理，以及纠纷解决等相关措施。

然而，阿里并未向用户告知“个人信息转移的国家”“接收个人信息的个人或法人的姓名（公司名称）及联系方式”等根据个人信息保护法规

定的应告知事项，也未在卖家须知中反映保护个人信息所需的措施。

（7）敏感数据泄露，T-Mobile 被罚 6000 万美元

2024 年 08 月，电信运营商 T-Mobile 因未能防止和报告敏感数据泄露事件，被美国外国投资委员会（the Committee on Foreign Investment in the U.S.，以下简称 CFIUS）处以 6000 万美元罚款，这也是该委员会有史以来开出的最大罚单。罚款金额之大，以及 CFIUS 前所未有地决定公开此事，显示该委员会正在采取更强硬的执法方式，以阻止未来可能发生的违规行为。

CFIUS 实施的处罚与 T-Mobile 违反了在 2020 年以 230 亿美元收购美国 Sprint 公司时与该委员会签订的缓解协议有关。美官员透露，T-Mobile 的敏感数据泄露事件发生在 2020 年和 2021 年，该公司未能及时报告这些事件，延误了 CFIUSS 实施调查和缓解任何潜在危害美国国家安全的努力。

T-Mobile 在一份声明中表示，公司在与 Sprint 合并后的整合过程中遇到了技术问题，影响了“少量执法信息请求中共享的信息”。该公司强调，这些数据从未离开执法部门，并且已“及时报告”和“迅速解决”。

（8）2024 年最高罚单！ Uber 因违反 GDPR 被罚 2.9 亿欧元

2024 年 08 月，GDPR 罚款“单王”诞生。荷兰数据保护局（DPA）对全球出行巨头优步（Uber）开出了一张创纪录的罚单，罚款金额高达 2.9 亿欧元（约合 3.24 亿美元）。罚款原因是优步在将欧洲出租车司机的个人数据传输至美国时，涉嫌未能遵守欧盟严格的数据保护标准。

> 综合来看，某些比较发达的国家对于企业违规的罚款金额是相当惊人的。某些国家开出的千万美元、上亿美元的罚单，的确可谓“天价罚单”。

荷兰 DPA 表示，优步在数据传输过程中未能适当保护司机的敏感信息，严重违反了《通用数据保护条例》（GDPR）的规定，同时也暴露了优步在数据保护方面的重大疏漏。据悉，优步在美国的服务器上存储了司机的敏感信息超过两年，包括账户详情、出租车执照、位置信息、照片、支付详情和身份文件。在某些情况下，这些数据甚至包含司机的犯罪记录和医疗信息。

（9）供应商泄露用户信息，AT&T 被罚近 1 亿元

2024 年 09 月，美国联邦通信委员会（FCC）与 AT&T 就 2023 年 1 月发生的重大数据泄露事件达成了一项 1300 万美元的和解协议。该事件源自 AT&T 的一家第三方云服务供应商。FCC 调查认为，该供应商未能按时删除数据并泄露，FCC 要求 AT&T 严格落实审查责任。

此次数据泄露导致 AT&T 超过 890 万名移动客户的信息被窃取。根据和解协议，一家未具名的公司，负责为 AT&T 提供用于营销、账单处理和生成个性化视频内容的服务，是此次事件的罪魁祸首。协议中提到，AT&T 为了使用这家供应商的服务，与其共享了包括用户数据在内的大量客户信息。

AT&T 与该供应商之间签署的合同中，明确规定了对这些数据进行保护和处理的要求。2016 年至 2020 年间，经过多次审查和评估，表明该供应商遵循了数据删除政策。然而，在 2023 年 1 月的泄露事件中，本应在 2017 年或 2018 年删除的数据被盗。FCC 最终认定，AT&T 对这一失误负有不可推卸的最终责任。

（10）明文存储用户密码，美国互联网巨头被罚超 7 亿元

2024 年 9 月，爱尔兰监管机构对 Meta 公司（Facebook 母公司）处以 1.01 亿美元（约合 7.08 亿元人民币）的罚款，原因是 Meta 以明文形式存储了数亿用户密码，并允许公司内部员工广泛访问这些密码。

Meta 早在 2019 年年初就披露了这一疏漏。该公司表示，旗下多个社交网络应用程序在记录用户密码时，

集体维权，在国内非常少见，
但在国外，特别是在欧美国家则时有发生。
网络安全事件也不例外。

使用了明文存储的方式，并将这些密码存储在了一个数据库中。该数据库被大约 2000 名公司工程师查询过，查询次数累计超过 900 万次。

爱尔兰数据保护委员会副专员 Graham Doyle 说：“鉴于访问这些数据的人可能会滥用数据，大家普遍认为用户密码不应以明文形式存储。我们必须考虑到，在这个案件中被讨论的密码尤为敏感，因为它们可以用于访问用户的社交媒体账号。

（11）泄露全球数亿人信息，国际酒店巨头万豪被罚超 3.6 亿元

由于 2014 年至 2020 年期间发生的多起重大数据泄露事件，影响了全球超过 3.44 亿人，2024 年 10 月 9 日，万豪宣布同意支付 5200 万美元（约合 3.67 亿元人民币）罚款，并制定一项全面的信息安全计划。

这是当日宣布的两项和解协议之一。第一项是万豪与美国 49 个州总检察长及华盛顿特区组成的联盟之间达成的和解协议。这一联盟在网络入侵者窃取了包括部分财务信息在内的敏感客户信息后发起调查。该笔 5200 万美元赔偿将分配给所有 50 位联盟成员。

第二项是万豪与美国联邦贸易委员会（FTC）达成的和解协议，要求万豪国际及其子公司喜达屋酒店及度假酒店国际集团（以下简称“喜达屋”）在未来 20 年内实施更严格的网络安全措施，并向 FTC 证明其合规情况。此外，万豪还需为客户提供便捷的方式，允许他们请求删除酒店已收集的个人信息。

（12）四家上市公司因网络安全信披违规被罚 5000 万元

2024 年 10 月，美国证券交易委员会（SEC）宣布，因四家公司在 2019 年“太阳风”（SolarWinds）数据泄露事件中做出误导性披露，决定对其处以民事罚款。被处罚的四家公司分别是网络安全公司 Check Point（罚款 99.5 万美元）、Mimecast（罚款 99 万美元），科技公司 Unisys（罚款 400 万美元）和 Avaya（罚款 100 万美元）。

这些公司均为“太阳风”黑客攻击的受害者，该攻击影响了多个使用“太阳风”软件的公司和政府机构。根据 SEC 的说法，四家公司都存在不同程度的违规行为，它们“敷衍了事”地淡化了这些攻击带来的损害。

SEC 执法部门代理主管 Sanjay Wadhwa 表示：“虽然上市公司可能成为网络攻击的目标，但它们有责任通过准确披露网络安全事件，保护股东和公众投资者的利益，而非提供误

导性信息。在这起案例中，SEC 认定这些公司在相关事件上提供了误导性披露，导致投资者无法了解事件的真实范围。”

SEC 指出，四家公司各自存在不同的违规之处。Avaya 宣称黑客仅访问了“有限数量”的公司电子邮件，却未提及黑客还访问了“其云文件共享环境中的至少 145 个文件”。Check Point 在明知漏洞存在的情况下，仅以“泛泛之辞”描述了网络入侵和潜在风险。Mimecast“拒绝披露”被盗代码及公司加密凭证的数量，“企图淡化攻击的严重性”。Unisys 则将其“网络安全事件的风险描述为假设性的”，尽管该公司遭遇了与“太阳风”相关的两次攻击。

小结

综合来看，境外某些比较发达的国家对于企业违规的罚款金额是相当惊人的。和国内一般只有 5~10 万元人民币的罚款金额相比，某些国家开出的千万美元、上亿美元的罚单，的确可谓“天价罚单”。不过，从本文收录的案例来看，事后追责式罚款，并不是“天价罚单”产生的主要原因，反而是违反 GDPR，违规跨境传数据，以及安全事件处置不及时等具体的违规行为，更容易遭到“天价罚单”，而且越是知名的大公司，越容易遭到“天价罚单”。

3、罚单之外，还有集体诉讼和民事赔偿

集体维权，在国内非常少见，但在国外，特别是在欧美国家则时有发生，网络安全事件也不例外。比如，2024 年 9 月，因勒索攻击泄露患者敏感数据，美国医疗巨头 LVHN 就被起诉赔偿了 6500 万美元。

利哈伊谷健康网络（Lehigh Valley Health Network，简称 LVHN）是美国宾夕法尼亚州最大的初级医疗集团之一。该机构于 2023 年 2 月 6 日发现其 IT 系统遭受入侵，随后确认臭名昭著的 ALPHV（又称 BlackCat）勒索团伙是这次攻击的幕后黑手。

勒索者共窃取了 13.4 万名患者和员工的相关数据，数据量达数 GB。这些被窃取的数据包括姓名、地址、社会安全号码、州 ID 信息，以及医疗记录和手术照片。勒索者要求 LVHN 支付赎金，否则将这些信息泄露到网上。

根据随后对 LVHN 提起的诉讼，该医院长期以来拍摄癌症患者的裸照。在某些情况下，甚至未经患者知晓。由于 LVHN 拒绝向 BlackCat 支付赎金，犯罪分子将部分资料发布到了网上，引发了客户的极大愤怒。

起诉书中指出：“虽然 LVHN 公开宣称他们勇敢地对抗了这些黑客，拒绝支付赎金，但实际上，他们忽视了真正的受害者。LVHN 并未优先考虑患者的利益，而是将自身的经济利益置于首位。”

3 月 4 日，ALPHV 团伙在其网站上发布了警告，威胁如果 LVHN 不支付赎金，他们将在线发布被盗的照片。LVHN 拒绝了这一要求，犯罪分子遂将部分窃取的资料上传至其暗网门户，其中包括带有个人身份信息的照片。

法庭文件显示，一名未具名的原告于 3 月 6 日接到医院合规副总裁的电话，得知她的裸照已被上传到网上。随后，这位副总裁“笑呵呵”地提供了两年的信用监控服务。这位匿名原告表示，她并不知情医院在她接受乳腺癌治疗时拍摄了她的裸照，更不清楚这些照片被存储在医院的企业服务器上。

尽管 LVHN 已通知客户和员工有关隐私泄露的情况，但 ALPHV 团伙继续加大压力，3 月 10 日再次泄露了 132GB 的数据，并威胁将每周继续泄露，直到赎金支付为止。

原告律师指出，医院未能履行其保护信息的责任，其行为还涉嫌违反了美国《健康保险可携性与责任法案》（HIPAA）。尽管 LVHN 同意了和解条款，但他们否认有任何不当行为。

2023 年 3 月，原告们正式对 LVHN 提起集体诉讼，指控这家医疗机构未能妥善保护患者数据。2024 年 9 月 11 日，原告代理律师事务所 Saltz Mongeluzzi Bendesky 宣布，已与 LVHN 就此集体诉讼达成 6500 万美元的和解。这家律所指出，“如果按每位患者计算，和解金额是医疗数据泄露勒索软件案件中最高的。”

那些数据被公开发布到网上的患者被分为四个等级。如果和解获得批准，最低等级的患者将获得每人 50 美元的赔偿。而最高等级（那些裸照被泄露的患者）在扣除律师费后，将获得 7 万至 8 万美元不等的赔偿。凡是收到 LVHN 通知的个人都将被视为集体诉讼的一部分，并自动获得赔偿，无需采取任何额外行动。

华云信安

以人才梯队为依托，以自主创新为核心，深耕网络空间安全产业

华云信安(深圳)科技有限公司（简称 华云信安™ ）成立于2016年，是一家深耕于网络空间安全领域，拥有自主研发能力及核心知识产权，提供网络安全解决方案与技术服务的高新技术企业。华云信安™总部位于深圳，在广州、上海、武汉设有分支机构，公司核心团队来自奇安信、网易、华为、绿盟、思科等国际知名科技企业，具有深厚的网络安全技术实力和管理经验。

华云信安™目前拥有数十项计算机软件著作权和十余款自主研发产品，具备“风险评估类”和“安全工程类”两项信息安全服务资质，通过ISO9001质量管理体系认证，现为深圳市信息安全行业协会理事单位和深圳市信息网络安全管理协会会员单位。

华云信安™凭借创新的网络安全产品体系、深厚的网络安全服务能力以及丰富的服务经验，为互联网、金融、能源、制造、交通、医疗、政务等领域的广大客户，提供专业优质的网络安全产品、网络安全解决方案和网络安全技术服务。

网络犯罪研究中心

华云信安·网络犯罪研究中心，是专注于打击网络犯罪的安全服务部门，致力于打击涉网新型犯罪领域的安全技术研究与产品研发，包括涉网犯罪案件技术支撑、网络诈骗案件技术支撑、涉众型经济犯罪案件技术支撑等，以攻防实验室和极牛技术社群组成创新型的安全研究团队，为国家及各省市公安机关提供高效专业的打击涉网犯罪情报分析服务和实战解决方案。

极牛攻防实验室

华云信安·极牛攻防实验室，由内部成员及外部知名技术专家团队组成，致力于最前沿网络安全技术的研究和调研，以指导技术研发路径和产品发展方向。其职责除开展传统的网络安全技术研究外，还跟踪国内外网络安全技术趋势并进行相关技术研究。现已协助国家互联网应急中心(CNcert)发现并修复数百个安全漏洞，获得数十张高危原创漏洞证明证书。

涉网犯罪对抗　护网重保服务　安全咨询服务　安全保障服务　安全培训服务

丰富的解决方案

我们提供卓越、丰富的信息安全产品及各行业解决方案、信息安全技术服务和基础架构咨询服务。

专业的团队服务

我们拥有资深、专业的服务团队，按需为用户提供多元化、多级别的咨询规划服务和技术实施服务。

众多的行业案例

我们拥有众多行业应用案例，包括制造、快消、航空、金融、物流、建筑、服务、互联网等行业。

深入的厂商合作

我们与多家国内外知名厂商建立战略合作关系，共同致力于优质解决方案及相关服务的推广落地。

全国范围的服务

我们公司总部在深圳，同时在上海、广州、武汉等设有分支机构，具有全国范围内的业务服务能力。

公众号 小程序 官网

网安观察

没有网络安全就没有国家安全

7436084028