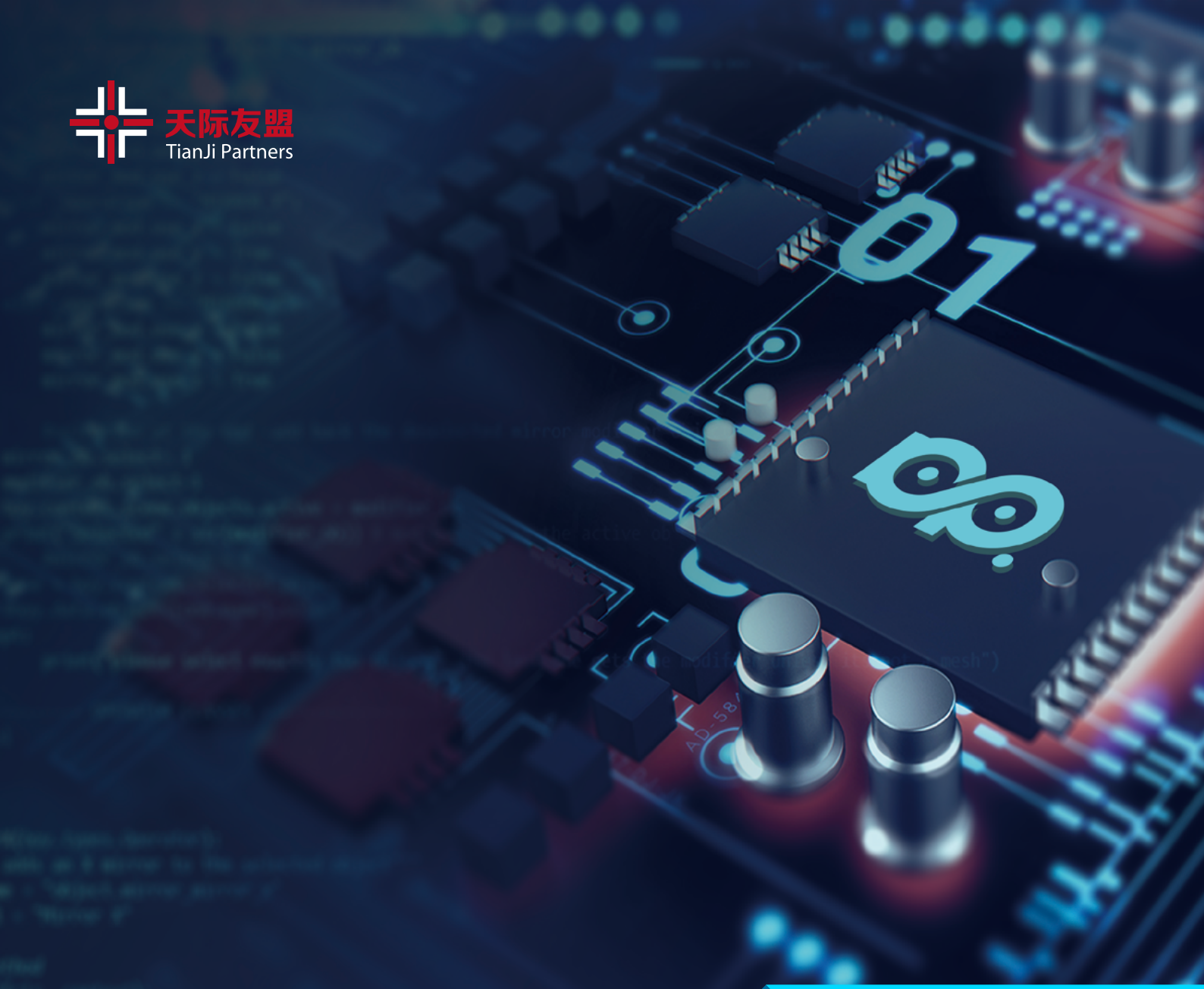
天际友盟
TianJi Partners



数字风险防护报告

Digital Risk Protection Report

2021 年度

2022-02

双子座实验室

前言

2021 年，跌宕起伏的新冠疫情成了一把双刃剑，在严重影响着人们日常生活的同时，也加速了全球数字化经济进程的脚步，企业越来越依赖社交和数字渠道来提高日常生产力、客户参与度和业务增长。由于这种依赖，企业需要保护这些渠道免受钓鱼仿冒、品牌侵权、数据泄露等风险。数字风险防护 Digital Risk Protection 的使命，即是保护现代企业免于遭受各种形式的数字威胁。

正确地应对数字化转型风险，可以让企业充分利用数字化转型技术，真正享受到数字化转型所带来的收益。越来越多的企业已经认识到保护其品牌、人员和数据的重要性。这将成为他们竞争优势的驱动因素。

然而，我们发现风险管理团队的能力已经难以跟上他们所要监管的数字化资产的增长，数字风险在覆盖范围和治理复杂度方面都超越了单个团队的能力，只有通过现代技术驱动的数字风险解决方案，才能帮助他们制定相应的应对策略。

2021 年 7 月，天际友盟凭借在数字风险防护领域的丰富积累，整理并发布了国内首份《数字风险防护报告》。该报告对 2021 年上半年度的国内数字风险态势进行了系统梳理，为各行业信息化和业务管理者提供了数字风险管理方法的思路和风险应对、决策制定所需要的态势数据。

数字风险态势呈现出速度、幅度变化的多样性，为了进一步帮助企业提高对其数字资产的保护意识，更好地抵御外部风险和威胁，天际友盟对 2021 年全年度的数字风险进行了完整的梳理和分析，希望对现代企业的数字风险应对有借鉴意义。

DRP
数字风险防护

contents
目录

01 数字风险概述

1.1 数字风险的社会背景

2021 年，跌宕起伏的新冠疫情早已成为一把双刃剑，在严重影响着人们日常生活的同时，也加速了全球数字化经济进程的脚步，加剧了各国政府应对这一进程的紧迫性。根据信通院发布的《全球数字经济白皮书》统计显示，2020 年，47 个国家数字经济增加值规模达到 32.6 万亿美元，同比名义增长 3.0%，占 GDP 比重的 43.7%。而 2020 年中国的数字经济发展突飞猛进，不仅增速是全球第一，市场规模也一再突破，目前已接近 5.4 万亿美元的规模，稳居世界第二位。数字经济核心产业在我国 GDP 中的比重也不断提升。借数字化创新，未来中国公司有机会成为改变全球竞争格局的关键力量。可见，数字化革新已成为我国，乃至世界各国发展经济的重中之重。

党中央也同样高度重视数字经济的发展。习近平书记指出，党的十八大以来，党中央高度重视发展数字经济，实施网络强国战略和国家大数据战略，拓展网络经济空间，推动互联网、大数据、人工智能和实体经济深度融合，建设数字中国、智慧社会，推进数字产业化和产业数字化。在此背景下，我国数字经济发展较快、成就显著。特别是疫情爆发以来，直播带货、在线医疗、在线教育、在线办公等数字技术、数字经济在支持抗击疫情、恢复生产生活方面发挥了重要作用。

数字技术的不断成熟，伴随而来的是数字风险的滋生。据估计，2022 年全球互联网流量将超过截至 2016 年的互联网流量之和。体量如此庞大且没有地域边界，网络空间势必乱象丛生，治理进程步履维艰。钓鱼欺诈、品牌侵权、社交媒体仿冒、勒索病毒以及数据泄露等数字威胁正在以各种各样的形式损害着企业与网民的权益。企业在面临各类风险时，由于缺乏足够的事前准备和有效的风险防护措施，碰到棘手问题时，通常手足无措、甚至延误解决问题的最佳时间窗口，不仅对自身品牌造成不可挽回的舆论压力，对消费者也有可能造成严重的直接经济损失。对此局面，Gartner 建议组织应建立新型“数字信任与安全”团队，专注于维护消费者与品牌之间的健全互动，同时向专业的服务团队寻求威胁应急支撑，以保证企业与消费者之间的正向持续沟通，最终实现品牌价值。内外防护机制的双重建立，对企业数字资产的保护是必要的选择。

1.2 国家监管的重视提升

随着互联网与人们生活工作的联系越来越紧密，网络信息治理也迫在眉睫。国家领导高度重视公民、法人和其他组织的合法权益。为了营造良好网络生态，近几年，我国相继发布了《网络安全法》、《网络信息内容生态治理规定》以及《互联网信息服务管理办法》等一系列法律法规，致力于维护国家安全和公共利益，构建天朗气清的网络环境。

同时，为了贯彻落实各项法律法规，国家相关部门进一步加大监管力度，对部分互联网龙头企业就互联网信息安全难题提出了整改要求。近日，工信部网络安全管理局、公安部刑事侦查局联合约谈阿里云、百度云两家企业相关负责人，通报了近期两家企业在防范治理电信网络诈骗工作中存在的接入涉诈网站数量居高不下等问题，要求其切实履

行网络与信息安全主体责任对相关问题限期予以整改；拒不整改或整改不到位的，将依法依规从严惩处。两家企业均表示将认真落实监管要求，进一步加强网站接入、域名注册、信息服务等管理，切实防范化解电信网络诈骗风险。

2021 年某企业美股上市将 APP 获取用户数据的尺度问题推到了风口浪尖。同年，CNCERT 会同网安协会联合建立了 App 收集使用个人信息监测平台、App 举报受理平台，并对 App 违法违规收集使用个人信息问题进行了总结梳理。据数据显示，隐私权限存在争议较大的几个知名应用商店为历趣应用市场、西西软件园、绿色资源网等。

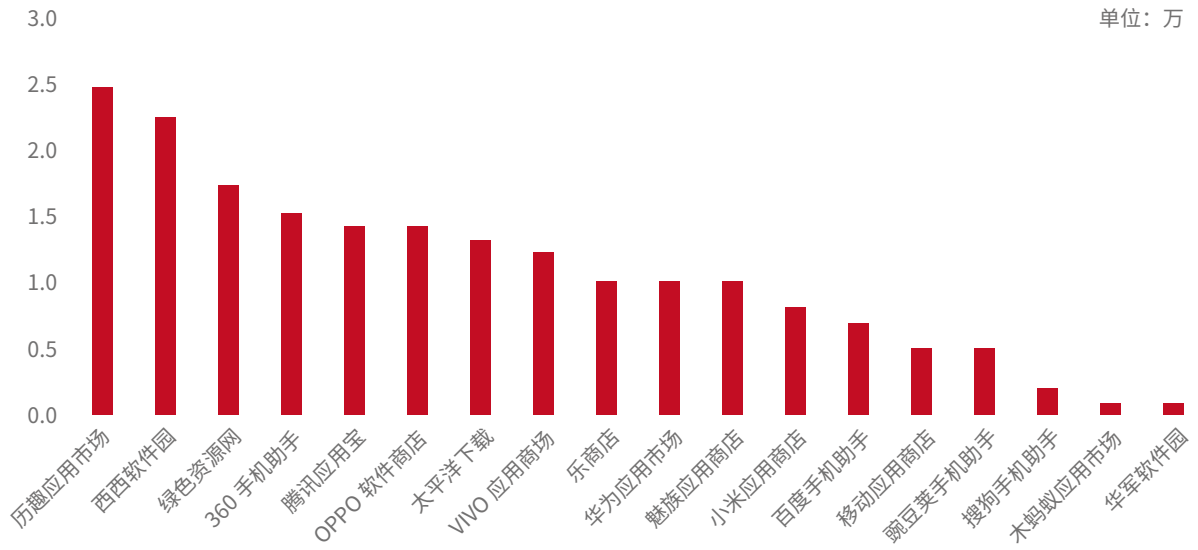


图 1：主流用应用商店 APP 同意隐私政策前收集个人信息问题分布情况

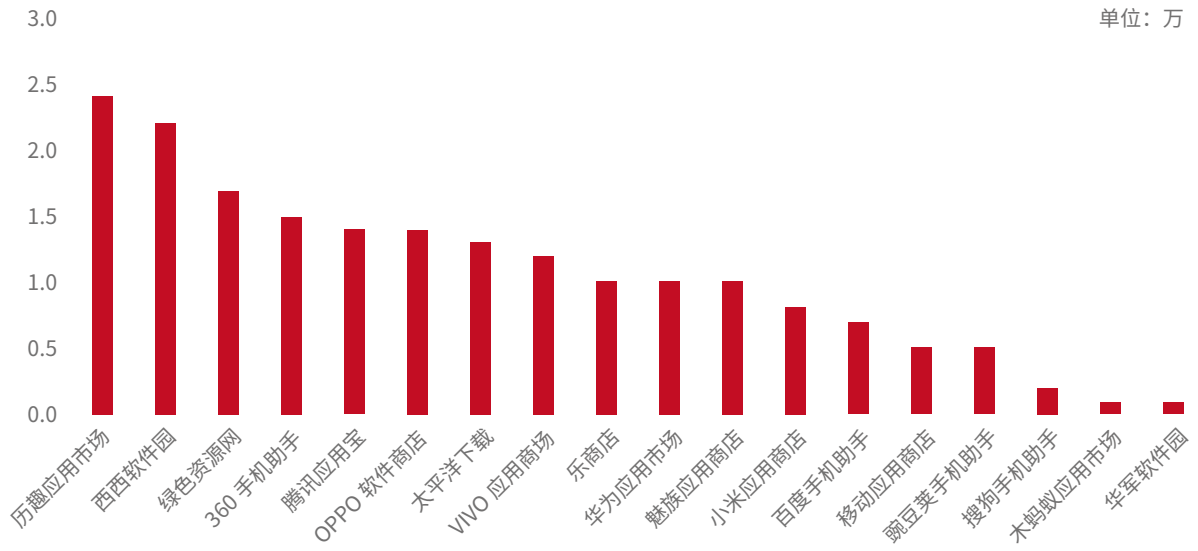


图 2：主流应用商店 APP 启动弹窗索要无关权限问题分布情况

加强对数字服务商的监管，维护国家互联网秩序，保障网民的权益，是全世界各国互联网执法部门的核心。一家主机托管服务公司的俄罗斯创始人 Aleksandr Grichishkin，因在 2008 年至 2015 年期间允许网络犯罪团伙使用其平台攻击美国多家金融机构而被判入狱 60 个月。运营期间，他为多起网络犯罪活动提供了分发恶意软件、托管网络钓鱼工具包、闯入目标网络、搭建僵尸网络以及窃取银行登录信息所需要的基础设施（包括 IP 地址、服务器和域名）等。据美国联邦存款保险公司（FDIC）估计，从 2011 年发生的安全事件来看，仅 SpyEye 攻击和 Zeus 攻击在单单一年内就对银行及其企业客户造成了大约 6400 万美元的损失。

由此可见，网络服务商的监管对于国家互联网治理的意义非同小可。

1.3 2021 年度数字风险监测范围

2021 年，天际友盟对国内外共 3,146 个品牌进行了数字风险监测。品牌共涉及金融、互联网、政府、大型企业、教育、版权作品、传媒、医疗、房地产、工业制造、国际贸易等十余个行业。

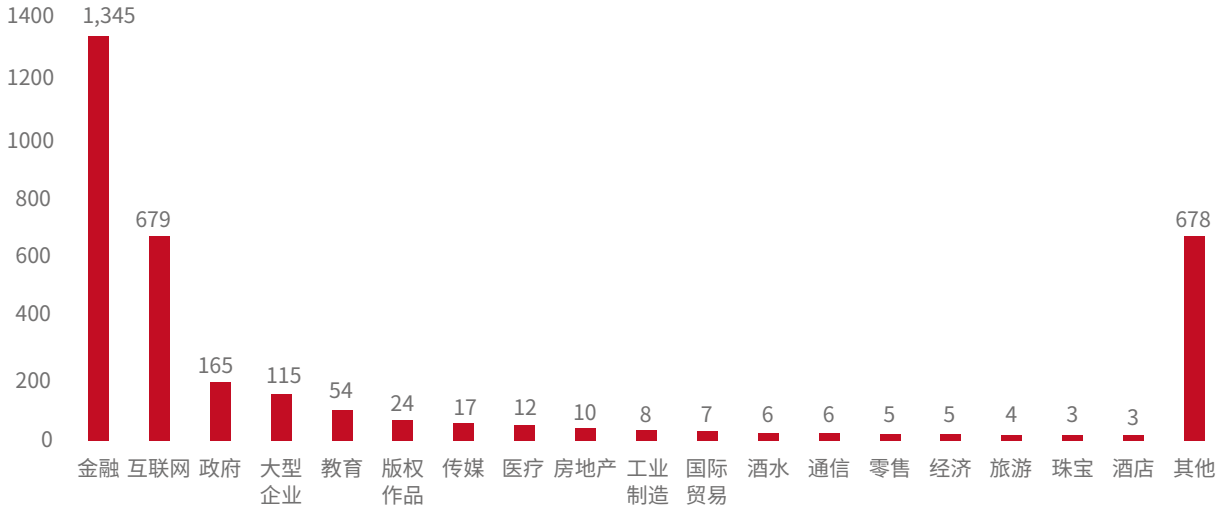


图 3：监测品牌的行业分布

行业	数量
金融	1,345
互联网	679
政府	165
大型企业	115
教育	54
版权作品	24
传媒	17
医疗	12
房地产	10
工业制造	8
国际贸易	7
酒水	6
通信	6
零售	5
经济	5
旅游	4
珠宝	3

酒店	3
其他	678
总量	3,146

表 1：监测品牌的行业分布

1.4 2021 年度数字风险主要特点

钓鱼欺诈

数字风险总量 NO.1

钓鱼欺诈的数量仍然“一骑绝尘”，领先于其他数字风险，这源于钓鱼欺诈可带来直接利益。在一定时期内，钓鱼欺诈仍将是数字风险的重点防范对象。

数据泄露

数字风险增长 NO.1

作为信息安全 CIA（机密性、完整性、可用性）的其中一个重点 C（机密性），网络安全失守带来数据的“双杀”困境，一是被加密勒索、二是数据泄露带来的多种衍生风险。数据泄露无疑会成为数字风险的一个大比例组成，且保持快速增长。

金融业

数字风险行业 NO.1

金融业由于行业的特性即风险管理，且直接与货币挂钩，因此始终是数字风险的重灾区，可以预见金融业作为数字风险的高发领域将长期保持不变。

数字风险网络服务商 NO.1	数字风险域名服务商 NO.1	数字风险国家 NO.1	数字风险社交媒体平台 NO.1	数字风险应用商店 NO.1
阿里云	GoDaddy	美国	微博	历趣
21.72%	16.76%	34.65%	39.85%	10.4%

数字风险的重点发展趋势有如下几点：

服务商集中化：某些云服务商刻意不作为，间接成为数字风险的最大帮凶，而云也成为数字风险的集中隐匿点。

风险场景多元化：各种可以直接或间接利益变现的手法，使数字风险发展出许多新的类型。

位置海外化：风险全球分布，寻求法律、监管的薄弱地区。

02 数字风险的评估

随着企业数字化转型，数字风险管理理论也在信息风险管理的基础上逐渐被企业管理者所认知。为了更好地研究数字化风险，在此引入 FAIR 模型的概念。FAIR 模型是信息安全领域广为使用的网络安全风险评估（CRA）框架。

FAIR（Factor Analysis of Information Risk 信息风险因素分析）模型的产生是为了减轻和预防由于大量企业依赖于高速发展的信息科技导致在复杂度呈几何级数递增的网络环境中出现了的棘手的网络安全问题。这些问题以数据泄露、品牌侵权、企业声誉受损等多种形式发生和存在，最终对企业造成直接和间接的财务损失。FAIR 模型对网络安全风险进行评估，帮助风险管理人员确定数字风险的优先级，分配有限的资源以缓解数字风险并做出进一步的防范决策。

2.1 FAIR 模型简介

FAIR 模型使用分类法将风险（财务损失）分解为风险因素，同时考虑了攻击者和防御者之间的能力竞赛，以及信息资产的脆弱性、攻击频率，并采用财务损失进行风险量化。FAIR 模型对风险因素之间的关系进行了以下描述。（见下图）：

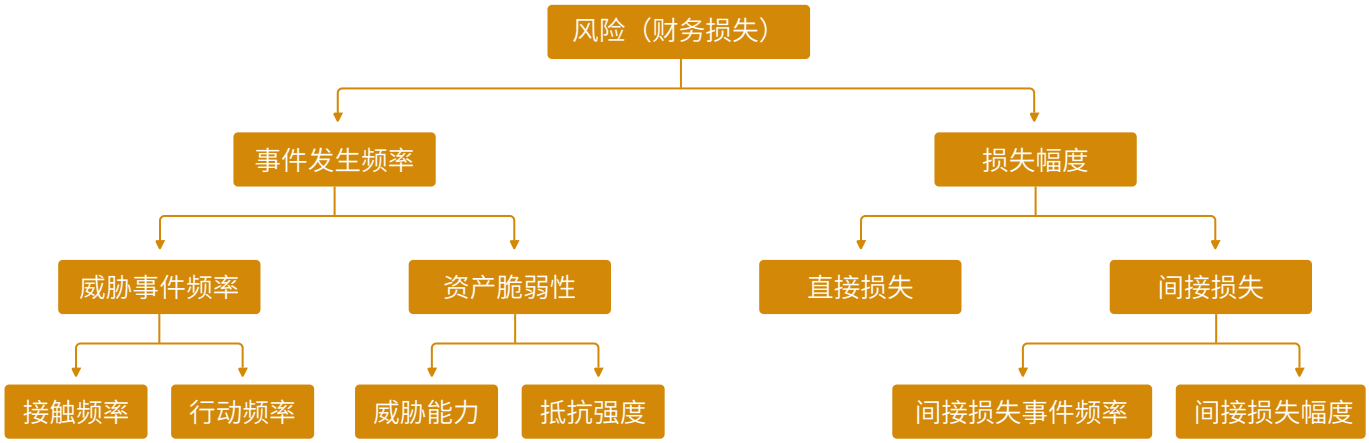


图 4：FAIR 模型

FAIR 模型对风险类别进行了建模。在风险分类时，风险因素需详尽无遗漏且各因素间呈互斥关系。整体风险（财务损失）由事件发生频率和损失幅度的乘积进行描述。 即：风险（财务损失）= 事件发生频率 * 损失幅度。

事件发生频率是指攻击者在给定时间范围内对信息资产造成伤害的频率，由威胁事件频率和资产脆弱性的乘积表达（事件发生频率 = 威胁事件频率 * 资产脆弱性），其中前者表示“攻击者对信息资产采取行动的频率”，而后者则被定义为“信息资产无法抵抗攻击者行动的可能性”。

威胁事件频率是攻击者与资产接触的频率，是攻击者一旦接触目标信息资产（接触频率）就会对资产采取行动的概率（行动概率），表达为：威胁事件频率 = 接触频率 * 行动概率。

资产脆弱性是威胁因素能够对资产施加的力量水平（威胁能力）与防御者对资产的控制强度（抵抗强度）之间的

差，表达为资产脆弱性 = 威胁能力 - 抵抗强度。

损失幅度由直接损失和间接损失共同组成，表达为：损失幅度 = 直接损失 + 间接损失。在 FAIR 模型中间接损失又称为次要损失，典型的例子有企业品牌负面影响、资金成本增加等。

间接损失可分解为间接损失事件频率和间接损失幅度，表达为：间接损失 = 间接损失事件频率 * 间接损失幅度。

综上所述，FAIR 模型完整的风险公式表达为：

风险 =（接触频率 * 行动概率）*（威胁能力 - 抵抗强度）*（直接损失 + 间接损失事件频率 * 间接损失幅度）。

2.2 数字风险分析模型（C-FADR 模型）简介

在数字风险的某些特定环境下，FAIR 模型具有一定的约束性。

信息资产公开性：在数字风险研究领域，主要被攻击对象为公开发布的应用系统，包括：企业网站、移动端应用、企业公众号和高级管理人员公众号，其典型表现为公开性。数字风险防护所提到的数据泄露概念，也是基于数字信息已经泄露的前提。

攻击能力易获性：由于开源测试软件的推广，各种测试软件和学习材料极其容易获取，而这些软件具有双面性，既可以用于应用系统的测试和改善，也可以被攻击者用于攻击行为，由于资产的公开性，针对网站、APP、公众号信息等展开的攻击行为可谓入无人之境。

威胁事件可测量性：针对数字风险的攻击，攻击者需要进行公开发布，方能产生攻击效果。因此通过对互联网、移动互联网、深网以及暗网的持续监测来感知威胁事件，并运用统计学原理进行计算，评估威胁事件的频率。故此，威胁事件具有可测量性，且测量过程可控、测量结果可信。

基于以上约束条件，数字风险的 FAIR 模型可简化为下图：

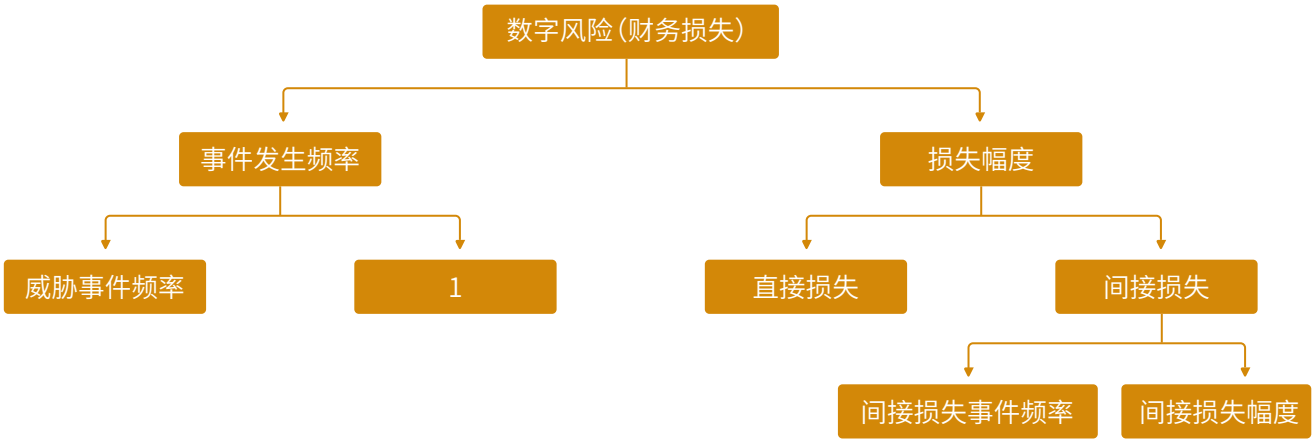


图 5：数字风险 FAIR 模型

由于上述模型的前提是针对威胁事件的测量和资产脆弱性的约束假设，因此，将该模型定义为约束的数字风险因素分析模型：Constraint-Factor Analysis of Digital Risk，简称 C-FADR。表达为：

数字风险 = 威胁事件频率 *（直接损失 + 间接损失事件频率 * 间接损失幅度）

经简化后的数字风险公式更加容易应用，企业可以通过监测互联网威胁和内部调查收集信息而快速完成风险评估。

2.3 损失幅度分析简介

2.3.1 防御者视角

在风险模型中，统计损失一向具有难度，尤其是当损失由直接损失和间接损失共同组成时。若间接损失犹如冰山隐藏在水下的部分，估算难度将更大。然而，通过科学的估算模型，间接损失仍然可以计算得出结果，甚至可以利用经验公式进行粗略估算，就如同利用密度比，结合冰山浮在水面上的部分去推算冰山整体体积一样。

针对数字风险所研究的范围，其直接损失将处于更小的比例。这里的直接损失是指，事件发生后，企业直接遭受的货币化损失，且损失数额可在损失前量化。数字风险的主要损失由间接损失构成。间接损失是指，在事件发生后可能会发生，其概率大于 0 且小于 1，具有一定或然性的损失。可能包括：

~ 民事、刑事或合同罚款和判决

~ 通知费用

~ 信用监控

~ 弥补二级利益相关者的金钱损失

~ 公共关系费用

~ 法律辩护费

~ 处置成本，由一线人员、公关、法务、其他相关人员的薪酬构成

* 监管制裁的影响

* 失去的市场份额

* 股价下跌

* 资金成本增加

以上间接成本，带有 ~ 符号的科目，企业可通过内部调研获得相对准确的数字，且误差可控。而带有 * 符号的科目，考虑到其影响的长期性、重要性、持续加强的非精准性等，需要投入相应的成本以获得更精准的数字。

2.3.2 攻击者视角

在上节中，本文采用了防御者的视角来分析数字风险，这也是风险模型中普遍采用的分析视角。然而，在某些场景中，仅采用防御者的视角分析风险并不全面，例如：针对政府网站的仿冒行为， 其损失往往无法简单地用货币化的直接损失 + 间接损失来衡量。这时候需要引进攻击者视角，所谓：“匹夫无罪，怀璧其罪”。采用攻击者价值视角，可以使企业和组织更加关注其社会责任。

由于针对数字资产的攻击可以直接或间接变现，且技术要求低、犯罪成本低、攻击者易藏匿于法外之处，因此分析攻击者能够获取有价值的情报信息，也使该模型成为分析非企业主体的首要参考模型。在此场景下，数字风险模型可被诠释为：

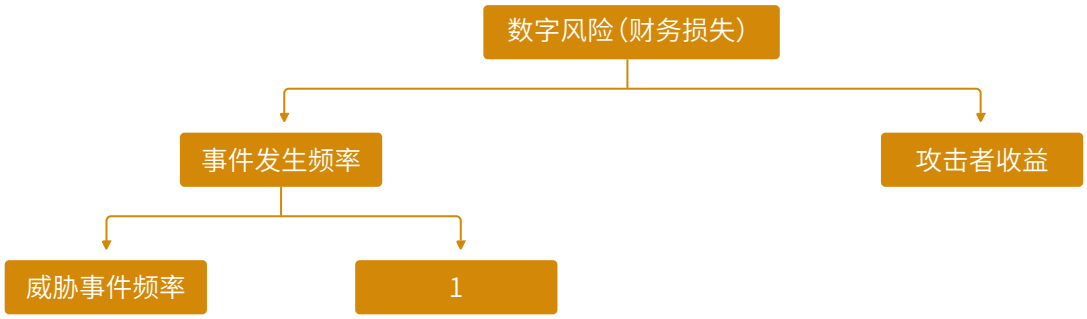


图 6：特定数字风险模型

其公式表达为：数字风险 = 威胁事件频率 * 攻击者收益。其中，攻击者收益可以通过公开信息进行分析。

2.4 数字风险管理的意义

数字风险是随着数字化转型而快速产生的规模化风险。经过精简和场景化后的数字风险模型可以帮助企业和组织应对数字化风险建模的挑战，重新定义信息技术风险的优先级矩阵，从而集中地、高效地管理应对数字风险的资源。

在建立数字风险模型之外，企业和组织还需要应对数字风险管理职责的挑战。在数字风险管理框架下，技术、风控、法务、市场等部门需在数字风险官（DRO）的统一领导下各司其职且多方协作，才能游刃有余地应对各种风险。

03 2021 年数字风险态势

3.1 按数字风险场景分类

常见数字风险场景可分为钓鱼欺诈，数据泄露，品牌侵权，威胁误报四大类。

2021 年的风险数据统计如下：

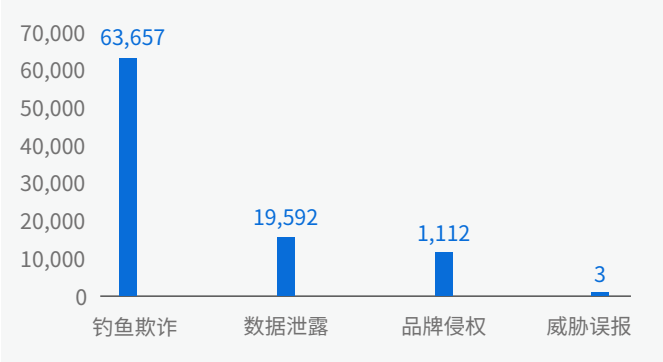


图 7：2021 年按风险场景划分的数字风险统计数据

场景类型	数量
钓鱼欺诈	63,657
数据泄露	19,592
品牌侵权	1,112
威胁误报	3
总量	84,364

表 2：2021 年按风险场景划分的数字风险统计数据

3.2 按资产类型分类

遭遇数字风险的常见 IT 资产包括网站，企业数据、移动 APP，版权作品、社交媒体账号、企业代码、及邮件等七类。2021 年的风险数据统计如下：

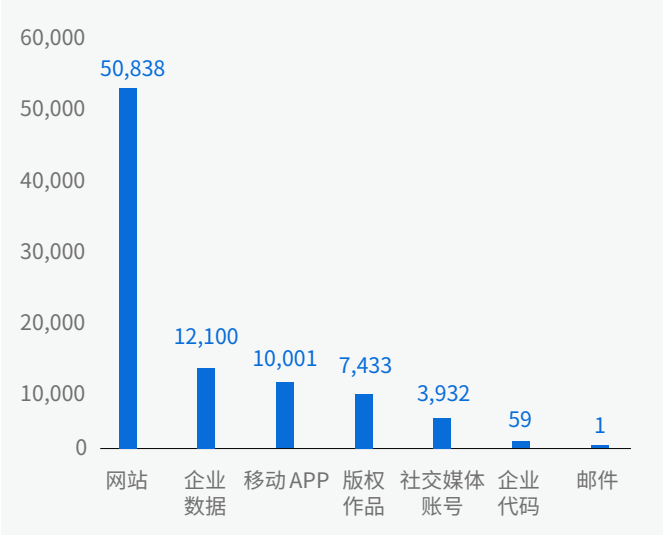


图 8：2021 年按资产类型划分的数字风险统计数据

资产类型	数量
网站	50,838
企业数据	12,100
移动 APP	10,001
版权作品	7,433
社交媒体账号	3,932
企业代码	59
邮件	1
总量	84,364

表 3：2021 年按资产类型划分的数字风险统计数据

3.3 按行业分类

各行各业都在数字化转型的过程中，因业务形态和发展阶段不同，数字风险聚焦程度也不尽相同，且会持续演进变化。根据统计，2021 年各行业的数字风险分布如下：

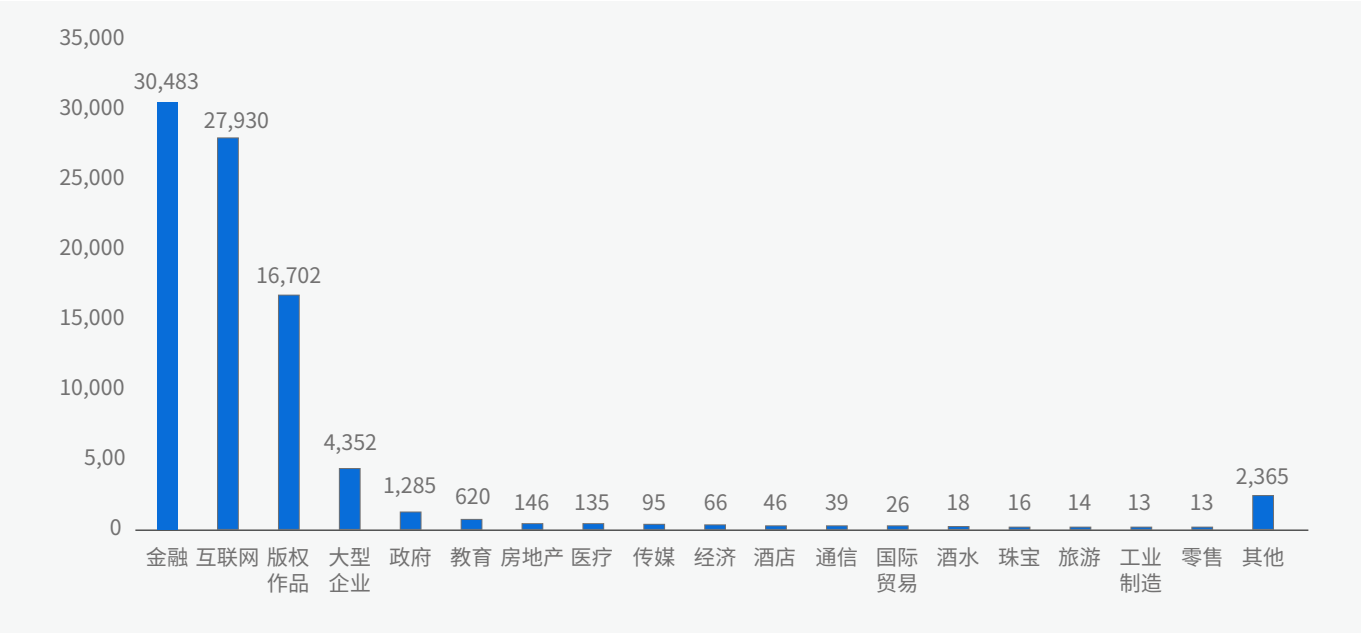


图 9：2021 年按行业划分的数字风险统计数据

行业	数量
金融	30,483
互联网	27,930
版权作品	16,702
大型企业	4,352
政府	1,285
教育	620
房地产	146
医疗	135
传媒	95
经济	66
酒店	46
通信	39
国际贸易	26
酒水	18
珠宝	16
旅游	14

工业制造	13
零售	13
其他	2,365
总量	84,364

表 4：2021 年按行业划分的数字风险统计数据

其中，金融行业可细分为如下几个子行业，各自的数字风险占比为：

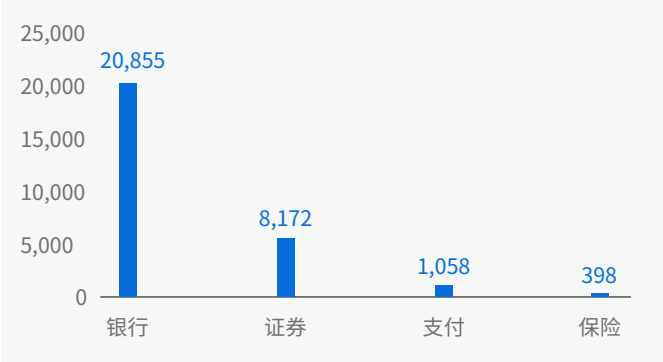


图 10：2021 年金融行业的风险数据

金融行业	数量
银行	20,855
证券	8,172
支付	1,058
保险	398
总量	30,483

表 5：2021 年金融行业的风险数据

互联网行业也可进一步细分为如下几个子行业，各自的数字风险占比为：

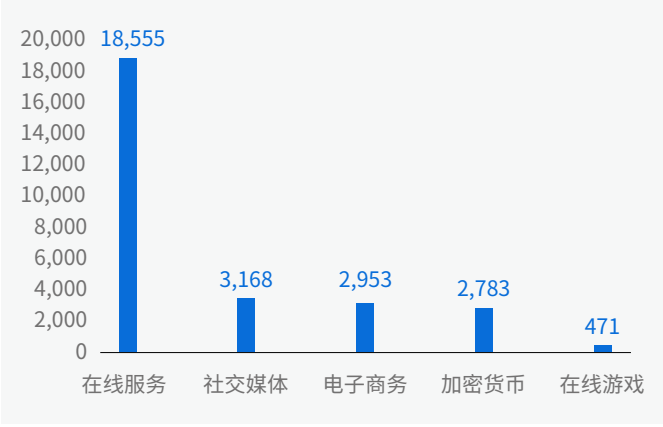


图 11：2021 年互联网行业的风险数据

互联网行业	数量
在线服务	18,555
社交媒体	3,168
电子商务	2,953
加密货币	2,783
在线游戏	471
总量	27,930

表 6：2021 年互联网行业的风险数据

04 2021 年数字风险溯源分析

4.1 按风险事件类型

4.1.1 银行金融信息钓鱼

攻击者利用钓鱼网站获取用户网络银行的登录信息以及银行卡信息，再结合补卡攻击等手段对用户银行账号和信用卡进行盗刷和盗转。

图 12：仿冒某银行的钓鱼网站示例

4.1.2 个人身份信息钓鱼

个人身份盗用常见于近几年来流行的贷款骗局，例如利用盗取的身份信息申请网贷，接着拨打诈骗电话使受害者上当，最终转出贷款。

图 13：某钓鱼平台盗取个人信息示例

4.1.3 企业认证信息钓鱼

企业认证信息钓鱼主要以企业为攻击对象。攻击者以“克隆”公检法等政府机构网站为主要手段，套取企业重要信息，用于各种企业身份认证、冒名开户、贷款等非法活动。

图 14：某盗取企业信息的钓鱼网站示例

4.1.4 利用官方 APP 蹭流量

通常，企业的官方 APP 只会发布到几大主流官方移动应用商店，比如苹果商店、华为应用商店等。但是由于安卓生态中的第三方商店繁多，很多商店运营者为了赚取流量，在未经授权的情况下将企业官方 APP 发布到其商店。此类行为会给企业品牌带来不小的安全隐患。且如果第三方商店被攻击，官方 APP 则随时面临被替换为恶意 APP 的可能。

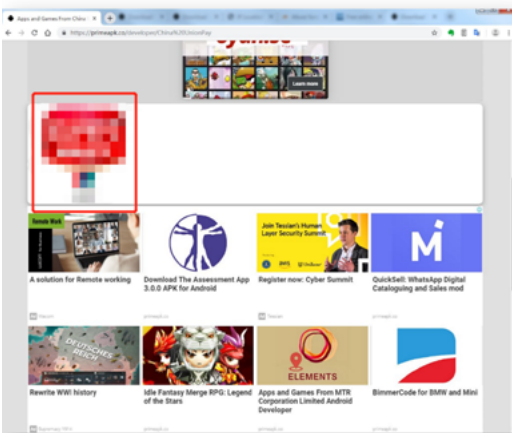


图 15：某 APP 未经授权传播示例

4.1.5 恶意 APP 钓鱼欺诈

攻击者利用企业的品牌知名度，对官方 APP 进行恶意篡改、重新封装，之后再通过钓鱼网站或野鸡商店来传播手机病毒或进行欺诈。此类恶意 APP 有时甚至和官方 APP 毫无相似之处，只是在网站页面盗用了品牌方的商标 Logo。

图 16：某恶意 APP 示例

4.1.6 利用品牌知名度引流或欺诈

利用知名品牌“蹭热度”的手法多种多样，比如宣称为品牌方授权合作伙伴来提高品牌的公信度，或者通过搜索引擎恶意排名来提高品牌曝光率，也有在非法的赌博、色情网站的源码中插入可信网站的代码，在躲避检测的同时还能进行引流。攻击者还可以把钓鱼、欺诈网页包装成某一知名品牌的相关页面，诱骗访问者输入敏感身份信息以及银行卡信息。

图 17: 仿冒某银行网站传播非法赌博示例

图 18：仿冒某外卖平台红包盗取信息示例

4.1.7 敏感资料泄漏

企业内部的资料和数据被前员工、供应商或者内部员工上传到代码、文档共享平台，甚至在这些平台进行售卖。有些泄露是内部员工为了工作方便的无心之过，有些则是恶意行为，这些都属于数据泄露风险的不同表现形式。即使不是恶意性质的攻击，但实际上已造成了机密或敏感文档可在公网被访问的结果，给企业带来一定程度的风险。

图 19：某航空公司季度报告被售卖

4.1.8 电子邮件欺诈

商业邮件欺诈，始终是全球恶意欺诈手法中的一大主流。欺诈者通过注册与客户主体接近的域名，并发送相关邮件，利用社会工程学技巧，进行仿冒和欺诈活动。与纯粹的电子邮件欺骗 (Email Spoofing，伪造电子邮件头，散播钓鱼网址链接或恶意附件) 不同，这类邮件欺诈往往更加隐蔽，目标通常是公司管理层或财务等核心部门人员，其欺诈目标和意图也更高，给企业带来的危害也更大。

图 20：仿冒电子邮件示例

4.1.9 影视版权盗版

版权是新时代数字作品的身份，但盗版一直是屡禁不止。不法分子直接窃取作者的成果，损害产业的良性发展生态。影视、小说、漫画、综艺等文化版权作品，遭到盗版和泄露，在各在线网站播放，严重影响版权的声誉和商业价值。

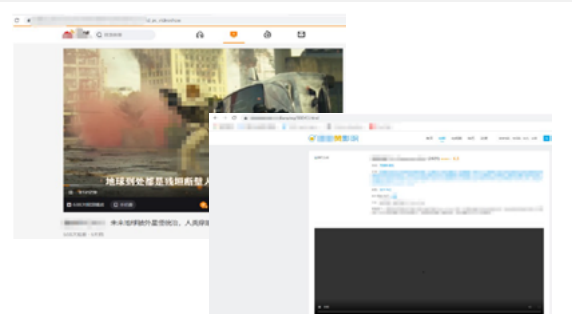


图 21：2021 年某好莱坞电影盗版资源示例

除传统影视文化作品外，体育直播等竞技类直播版权作品（比如 NBA、世界杯、UFC、电竞、赛车等），常年遭到盗链盗播，也同样严重影响直播行业的健康发展。

图 22：某盗版体育赛事直播网站示例

4.1.10 知识付费盗版

知识付费已经兴起多时，随之一起兴起的还有其盗版产业链。知识付费的主营业务交互完全依靠互联网平台来实现的行业，欺诈和损失也大都在线发生。大量不法分子通过高端技术手段非法获取正规平台的付费知识资产后，通过其他途径以低价出售。不少网民被优惠的价格所引诱，购买了盗版资源。这不仅对版权机构或版权者造成直接经济损失，同时也不利于建立积极正面的知识平台品牌形象。

图 23： 某知名美妆学院付费课程被盗版侵害示例

4.1.11 社交媒体仿冒

近几年，社交媒体已不仅是人们彼此之间用来分享意见、见解、经验和观点的工具和平台，越来越多的企业也借助社交媒体的力量，积极塑造企业的正面形象，积累品牌口碑，寻求与群众和消费者之间更紧密的触达点。而群众也深度依赖社交媒体平台来获取时下信息。但针对对象的官方性，大部分网民并不具备辨别能力。大量不法分子在社交媒体创建假冒企业账号、假冒企业员工或授权服务机构，试图获取用户信任，并骗取各类受害用户的银行卡账户、身份账号、各种密码等私密信息。

图 24：某仿冒人工客服的假客服示例

4.1.12 VIP 名人仿冒侵权

名人或企业高管的个人形象，是其最有价值的个人无形品牌资产，与企业品牌形象息息相关。当其遭遇风险时，同样会带来企业损失。社交媒体平台中存在的 VIP 仿冒账号，会利用民众信任，散步虚假消息或欺诈信息，不仅损害个人名誉，还可能引起公共事件，给企业造成进一步商业损失。

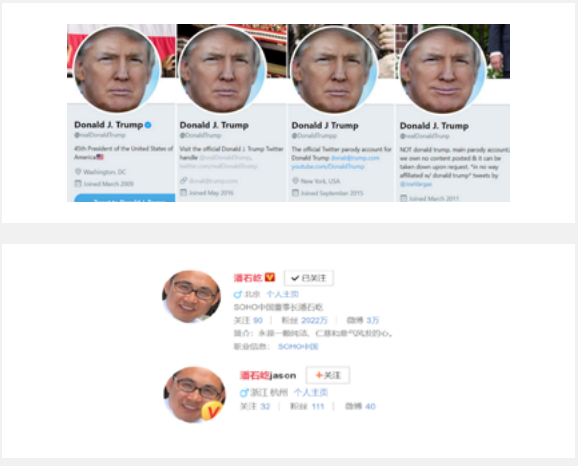


图 25：仿冒名人账号示例

4.1.13 企业内网代码泄露

互联网的普及和应用使办公效率得到显著提高，已成为企业发展中不可或缺的一部分。然而互联网带来便利的同时，也面临着外部的威胁。企业内部系统的源码中，往往会包含企业系统的配置文件，甚至密码等敏感信息，如果被泄露到第三方开放代码平台，攻击者可以进一步深入分析代码的逻辑漏洞，或用于钓鱼欺诈，公司被攻击和入侵的风险由此大大增加。

图 26：某企业内网代码泄露示例

4.2 按攻击团伙

4.2.1 金融欺诈团伙

金融欺诈团伙的主要目的是盗取银行金融、证券基金等在线服务的登录信息、银行卡信息，以及受骗者的个人信息（手机，身份证号，个人密码等），而后实施盗刷、盗转、诈骗、盗用身份等进行非法敛财行为。

对企业影响：

- 客户财产损失的风险
- 被上级部门通报批评，合规风险
- 大规模钓鱼攻击给企业带来的品牌名誉风险

金融作为第一大被攻击行业，攻击团伙还可以细分为如下几种类型：

4.2.1.1 大型银行钓鱼团伙

针对某些股份制大型银行的钓鱼仿冒，攻击者通常使用真实固定模板（只换 logo 和图片）。注册域名早期有一定规律，但逐渐趋于随机化。此类攻击仅针对手机用户，且仅对手机浏览器显示钓鱼内容。

图 27：仿冒某大型银行 APP 示例

4.2.1.2 城商行钓鱼团伙

活跃于 2021 年 2 月中旬至今，主要针对城商行进行钓鱼攻击，通常使用固定模板（只换 logo 和图片），具备一定的反侦测手段。页面加载时仅有一张图片，站内跳转至登录页面。此类操作提高了钓鱼网站的反爬虫性能。攻击仅针对手机用户，且仅对手机浏览器显示钓鱼内容。虽然时间较短，但是攻击力度非常大，我司侦测的数量已多达上万条。

图 28：仿冒某城商银行 APP 示例

4.2.1.3 证券基金交易所钓鱼团伙

此类团伙主要针对证券、基金、交易所等机构的钓鱼攻击。相对于上两种钓鱼手法，此类团伙使用的钓鱼模板基本固定。他们并不重视反侦测手段，但是攻击频率很高，且非常稳定。除一些知名的证券交易所之外，还会捏造一些疑似用于诈骗的虚构组织。例如：国金证券。

图 29：仿冒某证券交易所示例

4.2.2 同行恶意竞争

不同于纯粹的“犯罪团伙”，恶意竞争一般是由被攻击或者被仿冒品牌的竞争者发起。这种现象主要集中在加密货币、电子商务和在线服务等行业。通常发生的场景包括搜索引擎恶意排名和仿冒网站引流。

搜索引擎恶意排名：搜索引擎现在已经成为人们获取信息资源的主要途径之一。正是基于此，依照付费高低为标准的竞价排名服务也应运而生。竞价排名服务在给搜索引擎商带来盈利的同时，也日益暴露出了一些弊端，恶意排名正是其中之一。有些公司会利用同行业其他品牌的关键字来提高自身品牌的曝光机率，在搜索引擎上形成“货不对板”的现象。

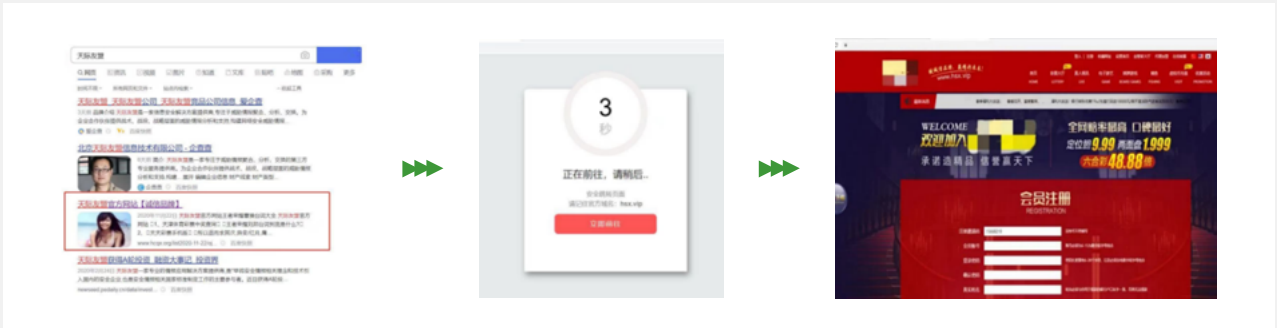


图 30：某搜索引擎恶意排名，链接转至非法赌博网站

仿冒网站引流：常发生在加密货币领域，新生事物总是会吸引很多人的眼球。我们也注意到有一些“后起之秀”，利用其他品牌的名声，创建仿冒网站，引流潜在客户到自己的交易所。

图 31：某数字货币交易平台假冒 APP

4.2.3 黄赌团伙

顾名思义，这类团伙的主要目的是传播色情网站和博彩网站。这两种网站是国家明令禁止的类型，但是为了利益，这类团伙想尽一切办法对这些网站进行传播。这类团伙有非常丰富的反侦测经验，通常利用银行、政府、大型企业等官方网站的网页代码作为掩护，对非法网站进行传播。这些非法网站大多数在境外托管，大部分并不触犯托管所在国家的法律法规，但是面向的“受众”和传播的方向仍是中国大陆的网民。

这类团伙除了对非法网站进行传播，还对那些被拿来“背书”的银行、政府、大型企业的品牌造成一些名誉上的影响。通过技术手段，正规网站的网站源码也被收录在非法网站的源代码中，造成搜索正规机构的关键字时，非法网站可能也排列在搜索结果之中。

图 32：仿冒某省政府网站传播足彩

4.2.4 恶意恐吓甲方团伙

恶意恐吓甲方是近年来发现的一个现象。

在钓鱼仿冒的打击中，除了与几个常见团伙持续对抗，也发现了一些不以攻击为目的的特别“团伙”。这些团伙会根据当前比较热点的钓鱼攻击，跟风注册一些有同样规律的域名，并且短暂地托管钓鱼仿冒网站。这些网站由于并未进行短信或邮件钓鱼传播，没有实际访问，因此并不会在“市面”流通，且生命周期极短，但是由于手法和规律与欺诈团伙相似同频，混杂在一起。

然而，经过我司分析，这些所谓的“攻击”，一般总会在甲方招标前期或者招标期间发生，数量虽然较大，但是没有实际欺诈行为，也不引流。因此，疑似是某些安全乙方企业为了吸引甲方关注获取经济利益而做出的“自产自销”行为。

4.3 按数字风险发生的平台

4.3.1 按社交媒体

社交媒体侦测数据涉及 19 个平台，下图按照每个平台的数量在总数中的占比，从大到小按顺序排列。其中微博占比最大为 39.85%。

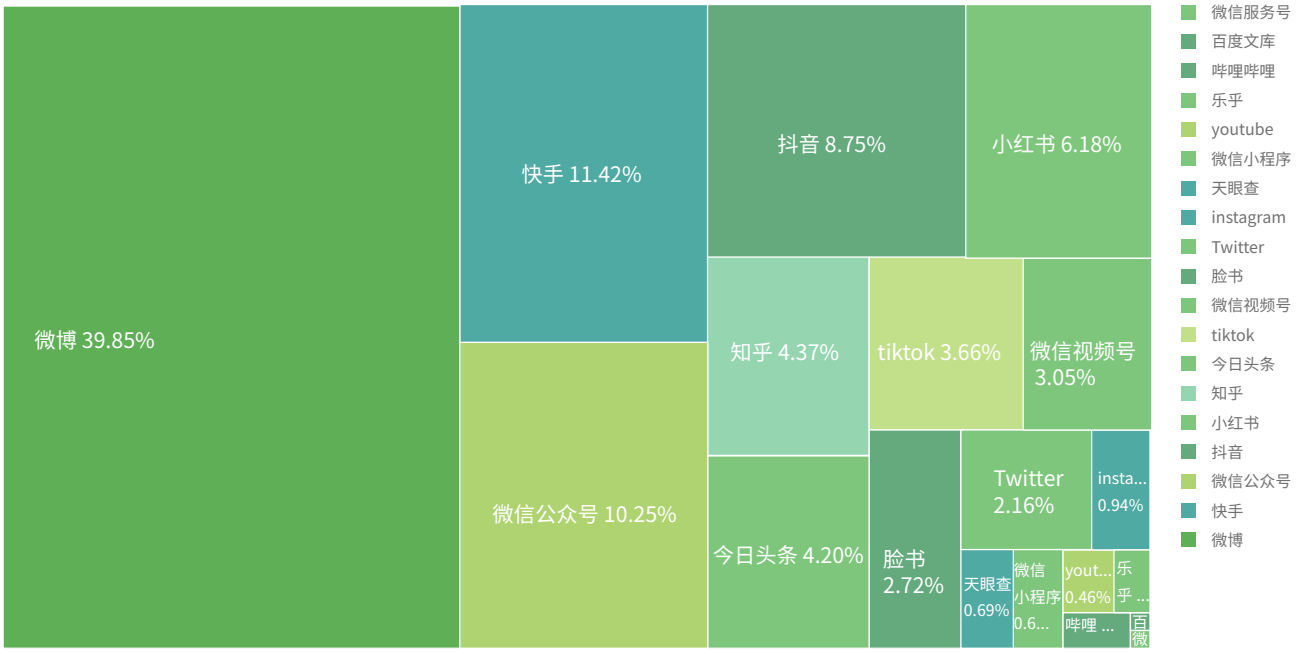


图 33：2021 年社交媒体发生的数字风险图示

平台	数量	占比
微博	1,567	39.85%
快手	449	11.42%
微信公众号	403	10.25%
抖音	344	8.75%
小红书	243	6.18%
知乎	172	4.37%
今日头条	165	4.20%
TikTok	144	3.66%
微信视频号	120	3.05%
脸书	107	2.72%
Twitter	85	2.16%
Instagram	37	0.94%
天眼查	27	0.69%
微信小程序	25	0.64%
YouTube	18	0.46%

乐乎	12	0.31%
哔哩哔哩	11	0.28%
百度文库	2	0.05%
微信服务号	1	0.03%
总量	3,932	100%

表 7：2021 年社交媒体发生的数字风险占比

4.3.2 按移动 APP 商店

移动 APP 商店 TOP30 占所有 APP 风险的 21.25%。以 TOP30 为整体，按百分比大小排列，其中历趣应用商店相对占比最多为 10.4%。

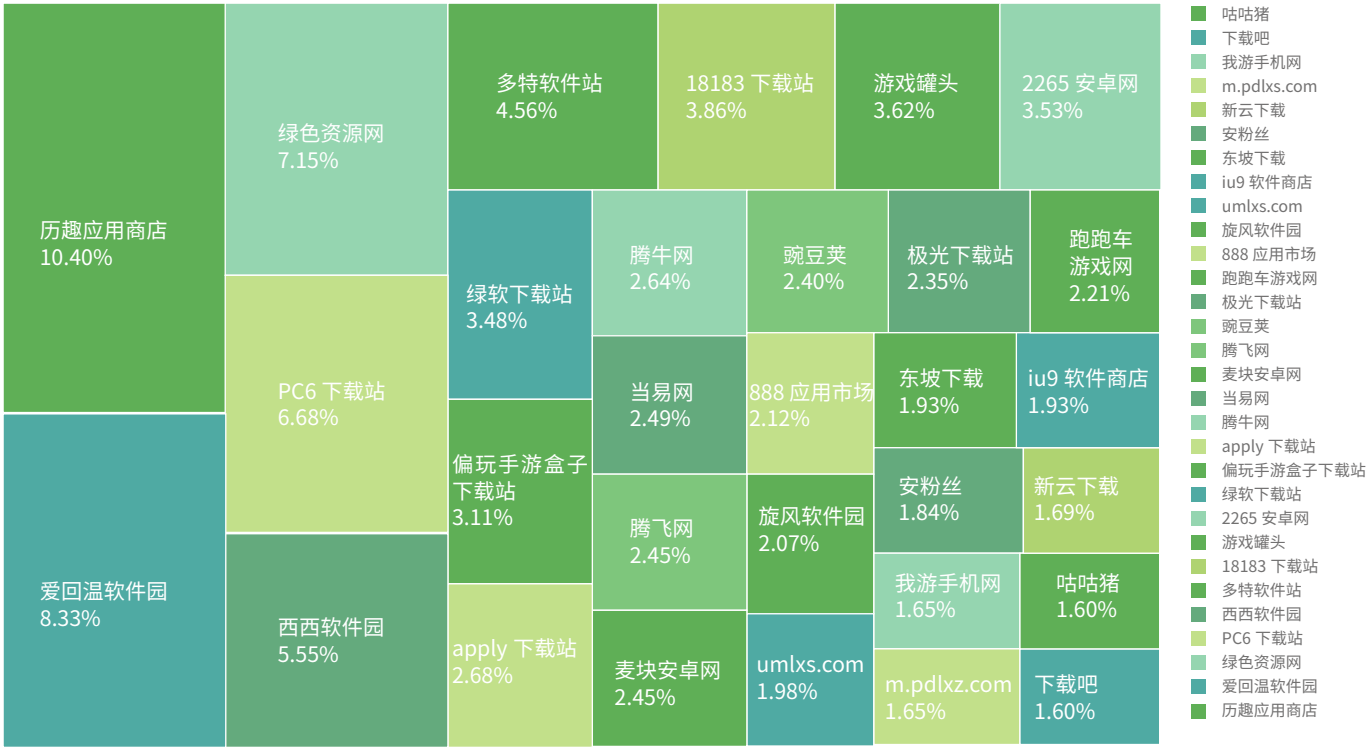


图 34：2021 年按移动 APP 商店划分类别的数字风险

应用商店	占比
历趣应用商店	10.4%
爱回温软件园	8.33%
绿色资源网	7.15%
PC6 下载站	6.68%
西西软件园	5.55%
多特软件站	4.56%
18183 下载站	3.86%
游戏罐头	3.62%
2265 安卓网	3.53%

绿软下载站	3.48%
偏玩手游盒子下载站	3.11%
apply 下载站	2.68%
腾牛网	2.64%
当易网	2.49%
腾飞网	2.45%
麦块安卓网	2.45%
豌豆荚	2.4%
极光下载站	2.35%
跑跑车游戏网	2.21%
888 应用市场	2.12%
旋风软件园	2.07%
umlxs.com	1.98%
东坡下载	1.93%
iu9 软件商店	1.93%
安粉丝	1.84%
新云下载	1.69%
我游手机网	1.65%
m.pdlxz.com	1.65%
咕咕猪	1.6%
下载吧	1.6%

表 8：2021 年按移动 APP 商店划分类别的数字风险占比

4.3.3 按网络服务商

从攻击团伙使用的 IP 所属的网络服务商来排序 TOP20，阿里云占比最高为 21.72%。TOP20 占总量的 68.59%。

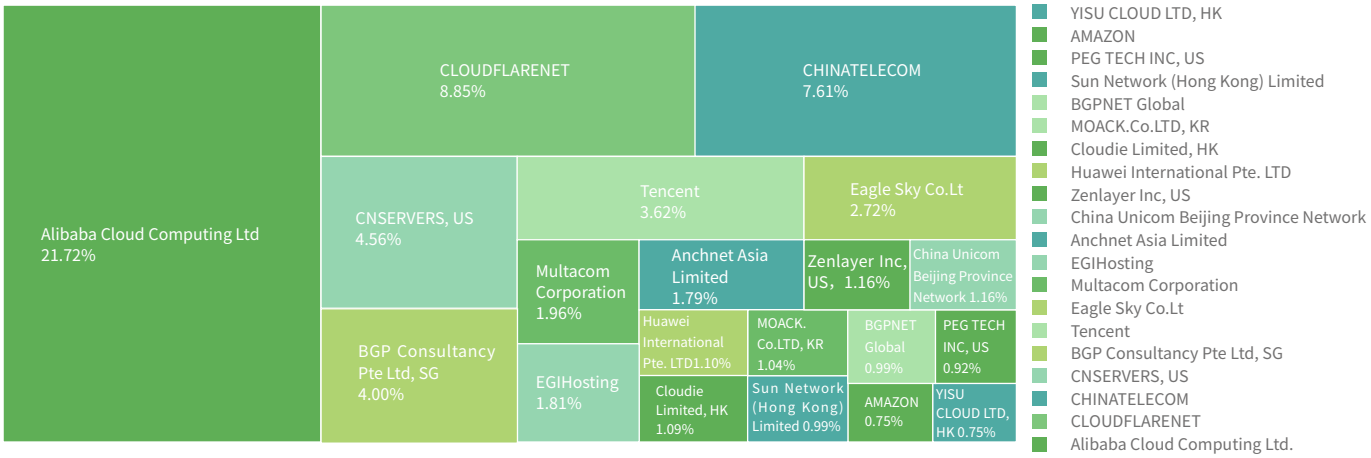


图 35：2021 年按网络服务商划分类别的数字风险图示

网络服务商	占比
Alibaba Cloud Computing Ltd.	21.72%
Cloudflare, Inc., US	8.85%
China Telecom	7.61%
CNSERVERS, US	4.56%
BGP Consultancy Pte Ltd, SG	4%
Tencent	3.62%
Eagle Sky Co.Lt	2.72%
Multacom Corporation	1.96%
EGIHosting	1.81%
Anchnet Asia Limited	1.79%
Zenlayer Inc, US	1.16%
China Unicom Beijing Province Network	1.16%
Huawei International Pte. LTD	1.1%
Cloudie Limited, HK	1.09%
MOACK.Co.LTD, KR	1.04%
Sun Network (Hong Kong) Limited	0.99%
BGPNET Global	0.99%
PEG TECH INC, US	0.92%
AMAZON	0.75%
YISU CLOUD LTD, HK	0.75%

表 9：2021 年按网络服务商划分类别的数字风险占比

4.3.4 按域名注册商

按主流域名注册商（TOP20）排列：其中 GoDaddy.com,LLC 占比最大为 16.76%，Alibaba Cloud ComputingLtd. 紧随其后。TOP20 占总量的 55.49%

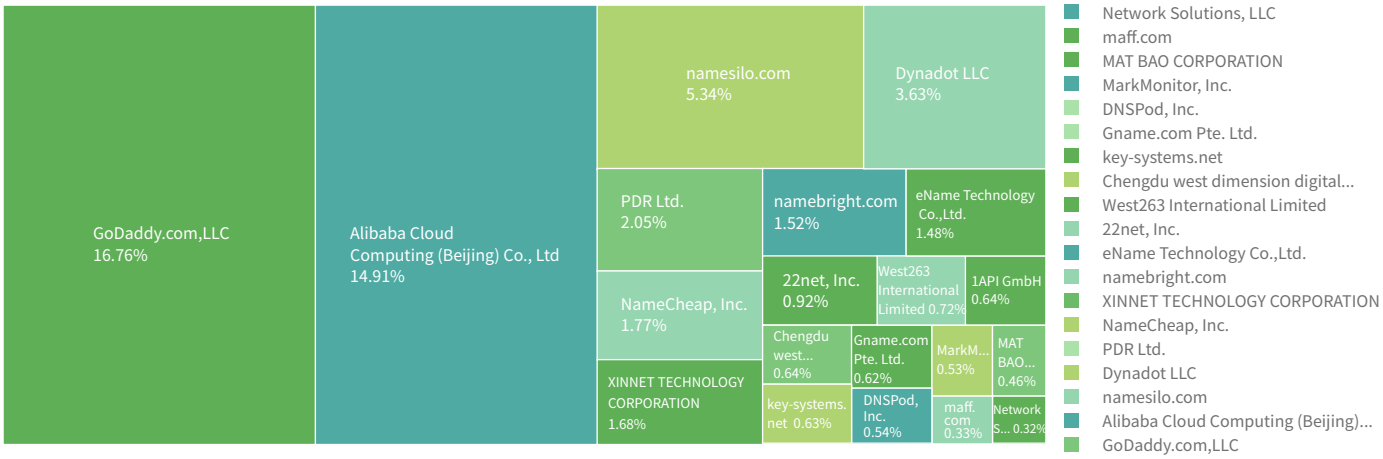


图 36：2021 年按主流域名注册商划分的数字风险图示

域名服务商	百分比
GoDaddy.com,LLC	16.76%
Alibaba Cloud ComputingLtd.	14.91%
namesilo.com	5.34%
Dynadot LLC	3.63%
PDR Ltd.	2.05%
NameCheap, Inc.	1.77%
XINNET TECHNOLOGY CORPORATION	1.68%
namebright.com	1.52%
eName Technology Co.,Ltd.	1.48%
22net, Inc.	0.92%
West263 International Limited	0.72%
1API GmbH	0.64%
Chengdu west dimension digital technology Co., LTD	0.64%
key-systems.net	0.63%
Gname.com Pte. Ltd.	0.62%
DNSPod, Inc.	0.54%
MarkMonitor, Inc.	0.53%
MAT BAO CORPORATION	0.46%
maff.com	0.33%
Network Solutions, LLC	0.32%

表 10：2021 年按主流域名注册商划分的数字风险占比

4.3.5 按照国家地区分布

按照攻击团伙使用的基础设施 IP 地理位置分布来看，各场景数字风险遍布 97 个国家和地区。下图将展示占比最高的前 20 个国家和地区，比例由高到低依次排列：

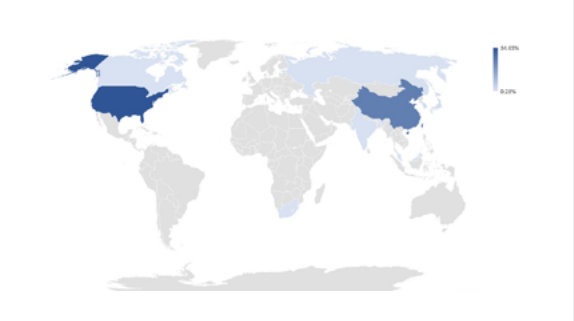


图 37：2021 年按世界地域划分的数字风险图示

国家和地区	数量	百分比
美国	25,996	34.65%
中国香港	18,356	24.47%
中国大陆	16,749	22.32%
新加坡	2,465	3.29%
韩国	1,518	2.02%
日本	1,337	1.78%
德国	924	1.23%
中国台湾	869	1.16%
印度	620	0.83%
荷兰	585	0.78%
印尼	577	0.77%
俄罗斯	574	0.77%
南非	452	0.60%
英国	427	0.57%
法国	381	0.51%
巴西	344	0.46%
泰国	337	0.45%
加拿大	297	0.40%
马来西亚	263	0.35%
澳大利亚	221	0.29%
其他 77 个国家和地区	1,737	2.32%

表 11：2021 年按世界地域划分的数字风险占比

05 数字风险典型案例

5.1 钓鱼欺诈及仿冒

5.1.1 网站

5.1.1.1 常见钓鱼网站

犯罪分子假冒某外卖品牌客服的口吻向用户发送要求商户认证的短信，内含钓鱼网站链接，诱导商户输入身份证、银行卡、手机号、验证码等信息，从而对商户银行卡进行盗刷，造成经济损失犯罪分子利用商户关注客诉处置、平台系统升级的心理，通过含有钓鱼链接的短信实施诈骗，受害者一旦输入相关个人信息，银行卡就会被盗刷，严重威胁人民群众财产安全。

图 38：公安部针对某品牌钓鱼网站发布的提示

图 39：以某品牌招商为由的钓鱼网站

图 40：以骗取用户信息为目的的仿冒某资本企业的钓鱼网站

5.1.1.2 新型勒索 URL

图 41：域名仿冒 URL 升级为 URL 勒索病毒

仿冒某投资公司的恶意网站将域名仿冒和勒索行为合二为一，不仅高度仿冒了企业的官网域名以混淆视听，同时对所有访问的且存在安全漏洞的 PC 进行强制锁定，从而以协助解锁为条件进行钱财勒索。安装防护软件的用户在同意安装插件后，PC 的文件同样会被强制锁定。后经处置，目前访问目标网站会跳转到其他网站，但均无法继续下载恶意程序。

5.1.2 移动 APP

5.1.2.1 APP 广告引流

图 42：某支付品牌 APP 未经授权上架

一应用商店未经授权上架了某知名支付 APP。下载并安装应用程序后发现，实际应用为 APK Downloader(一款伪造为应用商店，骗取用户点击为广告引流，获取广告费，实际并不产生任何下载行为)，尚未发现其他恶意行为。此外，深入调查该下载站点内所有 APP 均为同一 Adware APP(APK Downloader)，此 APP 的下载功能实则是为 google 广告引流而存在。该平台涉嫌仿冒官方 APP，属商标侵权行为。且网友暂未向品牌方举报被诈骗钱财的情况，故目前不涉及欺诈行为。处置后，侵权 APP 已下架，无法被搜索。

5.1.2.2 APP 仿冒

图 43：某云服务品牌 APP 未经授权上架

攻击者开发仿冒的企业 App，滥用品牌 Logo、商标，并通过未授权渠道分发下载，试图骗取各类受害用户的银行卡账户、身份账号、各种密码等私密信息。

5.1.3 社交媒体

5.1.3.1 微信账号仿冒

虚假的公众号（已进行企业实名认证），按微信规则，此类场景提交侵权证据后，可将公众号下线。

图 44：某交易平台的微信仿冒公众号

该案例是微信号而非公众号（未进行实名认证）。按微信规则，如果无法提供充分的欺诈证据，只能发出警告，要求对方去除侵权商标。通过处置后，该微信号删除了品牌方 LOGO，并去除了与其相关的内容。

图 44：某交易平台的微信仿冒公众号

5.1.3.2 小红书账号仿冒

某一小红书账号仿冒账号名称与某知名银行同名，存在品牌侵权行为。经处置后，该账号已修改为与品牌方无关的账号名称。

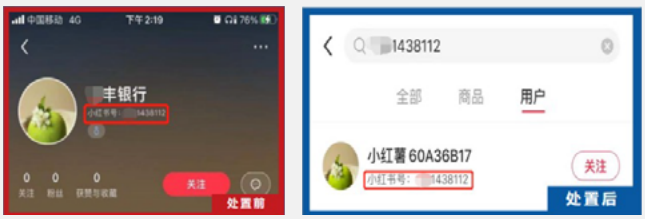


图 46：某银行在小红书上的仿冒账号

5.1.4 邮箱

5.1.4.1 官方邮箱被钓鱼

某知名物流企业的官方服务邮箱被黑客攻破，且被利用参与钓鱼行为。处置手段为或停止域名解析，或停止邮件服务。因服务邮箱与其大量客户关系紧密，故品牌方需经内部评估后再做决策，暂未进行处置。

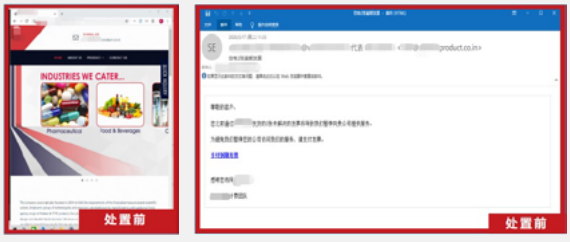


图 47：某物流公司的官方客服邮箱“被参与”钓鱼

5.1.4.2 域名相似的钓鱼邮箱

此案例中，犯罪分子使用的钓鱼邮箱与一知名短视频平台的官方服务邮箱高度相似该钓鱼邮箱发送有偿推广信息，哄骗用户点击邮件中嵌入的钓鱼网站，以窃取用户的私密信息、银行卡号等数据。后经处置，该邮箱的域名已被停止解析，网页无法访问；同时，涉事邮箱的邮箱服务也已被暂停，无法登陆。

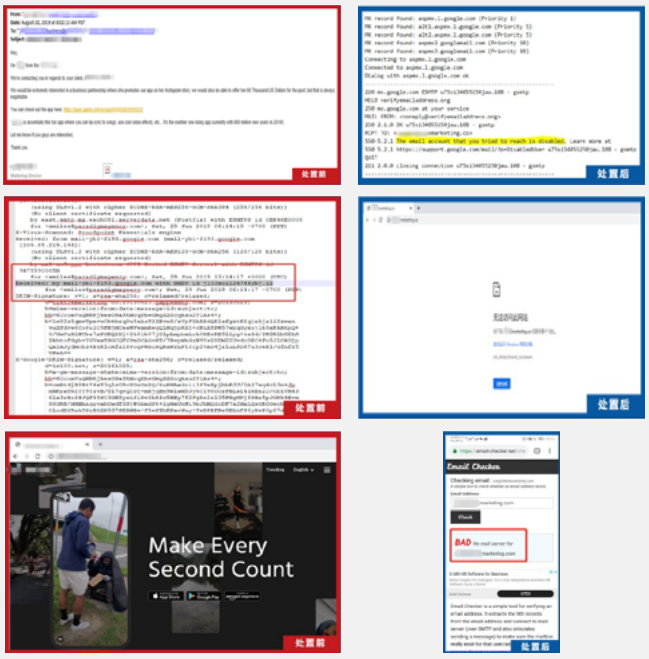


图 48：与某短视频平台官方客户域名相似的钓鱼邮箱

5.2 品牌侵权

5.2.1 网页

5.2.1.1 虚假宣传合作关系

侵权网站虚假宣传与某交易平台的合作关系（并使用了该平台的注册商标）。其主要目的是借用被侵权品牌的名誉为自身推广、大搞资金盘等行为。

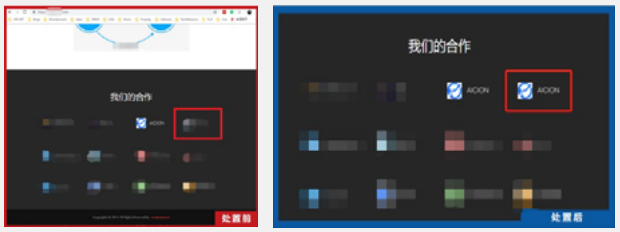


图 49：某品牌网站涉嫌虚假宣传，构成侵权行为

5.2.1.2 黄赌毒引流

侵权网站滥用了某短视频网站的品牌名称，为自身网站的黄色资源进行引流，对品牌方造成了不良影响，有损品牌形象。处置后，该页面内容已全部删除。

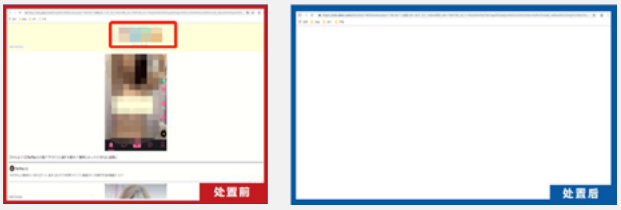


图 50：涉黄网站滥用品牌商标构成侵权

5.2.2 移动 APP

5.2.2.1 虚假宣传合作关系

不仅是网页，APP 也有可能被检测存在虚假宣传合作关系的行为。通常，在 APP 首页或下方位置展示关联组织，是品牌侵权的高发地。

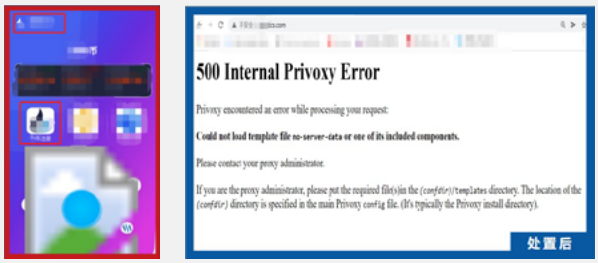


图 51：侵权 APP 滥用某交易平台商标并生成存在合作关系

5.2.2.2 “无中生有”的侵权 APP

杭州某公司接到网民举报有犯罪分子冒用其企业名义制作和发布金融投资理财 APP，导致不少网友被诈骗钱财。该公司发布声明辟谣从未建立过任何理财 APP，涉事 APP 属商标侵权行为。为了维护品牌形象，阻止更多网民发生经济损失。涉事品牌方已向公安机关举报。

图 52：某科技公司 APP 被仿冒

5.3 版权盗版

盗版资源的多种多样和与时俱进令人瞠目结舌。随着网络时代的来临，曾经的盗版书籍、杂志、影碟、软件安装盘等实体逐渐退出人们的视线，慢慢转型为数字形式重新进入大众的生活。虽然这种数字化转型很大程度上为品牌方和用户提供了便利，减小了互动成本，但盗版问题也随着互联网的发展潜滋暗长，并愈演愈烈。影视、综艺、赛事、音乐、办公软件、游戏、摄影等等均未能幸免于难。以受灾最为严重的影视为例，从多年前的盗版影碟到如今关注公众号获取资源链接，盗版问题一直困扰着实体和数字领域。

5.3.1 在线影院

自互联网进入大众视野的那天起，各种在线影院始终是网民获取盗版资源的主要方式之一。这类网站的创建和维护均不需要高深的技术能力，同时经济成本低，广告收益大，很受不法分子的追捧。通常网络上有此类站点的搭建模板。

图 53：某国际电影的在线影院盗版资源

5.3.2 网盘下载

网盘的兴起为网民之间的资源共享带来了极大的便利，但也为盗版资源的传播提供了渠道。用户可通过网盘下载大容量的高清片源来提高观影质量。这些片源如果在线观看则有可能受网速限制导致进度受阻，观影体验则大打折扣。

图 54：某国际电影的网盘盗版资源

5.3.3 BT 下载

BT 种子下载在多年前曾风靡一时，但如今随着互联网的发展，各种新型平台的出现，BT 种子虽常见于贴吧论坛，但地位早已一落千丈。原因有很多种，其中之一在于受限的下载速度。下载软件为付费会员提供了高速下载，但会员费价格不菲。经费不足的网友可能会花上一两天或是更久的时间才能看到自己心仪的影片，但彼时的观影心情已严重受挫。

图 55：某国际电影的 BT 盗版资源

5.3.4 社交媒体

社交媒体的盗版资源不仅轻易获取，且利用了其平台的特性，结合了用户的碎片时间，吸引了很多网民的眼球。社媒突破了其他平台的时间和地域限制，赋予了网民最大程度上的观影自由。无论在哪里，只要用户时间允许，即可获得观影体验。

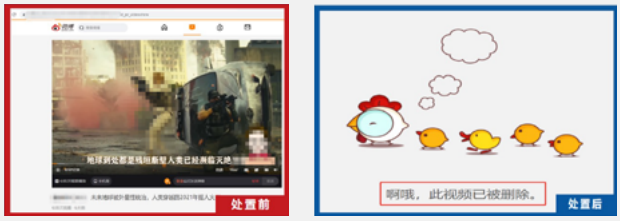


图 56：某国际电影在社交媒体上的盗版资源

5.4 数据泄露

5.4.1 文库

各类文库平台是泄露数据大肆传播的重灾区之一。大量上传者以付费浏览或下载的方式对企业机密文件进行不正当牟利。这不仅损害企业的声誉，同时对其技术成果、项目业绩都将造成严重威胁。

图 57：某科技公司的可报告模板被泄露在某文库平台

5.4.2 网站

部分发生在网站的数据泄露并不是以公开下载的文档形式进行传播，而是直接在网站上公布泄露内容，以吸引网友的流量。

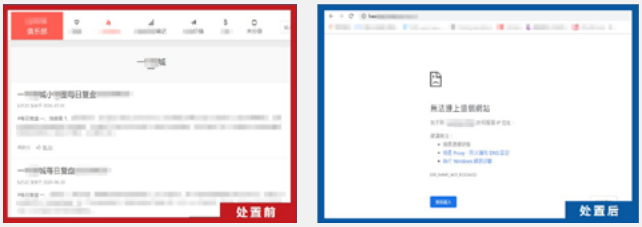


图 58：某知识平台的付费内容被公开发表在某网站上

5.4.3 网盘

企业用户信息、市场战略、技术发明等核心内部资料，遭到非法窃取，并公开在网盘等平台传播，不仅直接导致企业利益受损，还会影响企业安全和品牌声誉。

图 59：某企业实施方案被泄露在网盘上

5.4.4 知识付费

新冠肺炎疫情期间，在线教育行业与知识付费需求激增，为头部品牌打响了知名度。但相关的低价文档也猖獗起来，数千上万元的网课，被放到山寨或知识分享网站和论坛中，然后通过闲鱼、百度贴吧等平台进行售卖，只需要几十元便可购得。严重影响了平台方的会员计划和商业回报，也打击了知识生产者的创作热情。

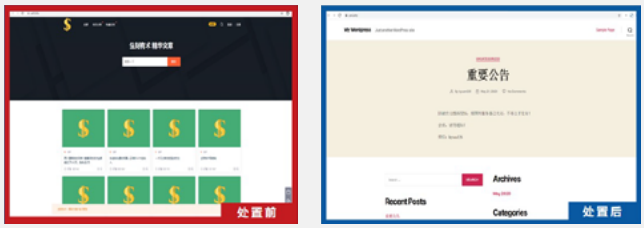


图 60：某知识平台的付费文章被另一知识平台盗用

5.4.5 社交媒体

很多不法分子利用社交媒体来传播正版付费内容，企图扩大与网友的接触面。同时，该类行为不仅为付费内容版权方造成业务损失，更会损害其品牌形象。

图 61：某网课在微信上被公开售卖

5.5 代码泄露

5.5.1 Github 平台的代码泄露

某银行涉及线上售后退货服务的代码数据被公开分享至 Github 平台。被公开的代码不仅有可能会被恶意人员所利用，对品牌的服务系统进行攻击勒索，更存在对广大消费者造成经济诈骗，严重影响品牌形象。后经处置，泄露代码已在 Github 平台下架。

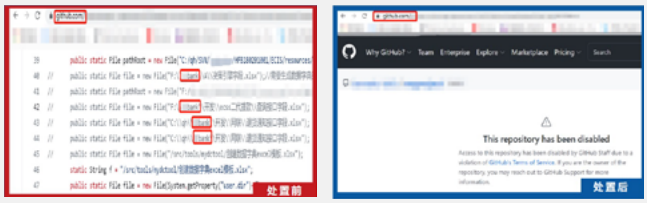


图 62：某银行的内部代码被分享在 Github

5.5.2 Gitee 平台的代码泄露

Gitee 是另一个代码泄露的高发地段。某银行内部视频会议软解接口代码在 Gitee 平台上架并免费浏览。外部威胁可轻而易举利用代码漏洞对银行的重要会议进行监测或监控，获取参会人员的网络数据，造成严重是网络安全危机。后经处置，涉事代码已被下架。

图 63：某银行的视频软件代码被分享在 Gitee

5.6 威胁误报

5.6.1 网页威胁误报

5.6.1.1PC 端

腾讯安全监测某品牌方的官方网站存在风险，且标记为危险。通过与腾讯安全中心交涉，该站存在被恶意举报的行为，通过处置沟通该站恢复。期间涉及腾讯安全的审查工作周期是自提交审核日起，30 工作日后恢复误报。

图 64：腾讯安全中心误判某品牌官网存在风险

5.6.1.2 移动端

华为手机内置的华为浏览器，各版本均对某交易平台官网误报为威胁对象。通过沟通处置后，威胁误报在 15 个工作日后得到恢复。

图 65：华为手机浏览器误判某品牌官网存在风险

5.6.2 移动 APP 威胁误报

某品牌官方手机网页提供的 APP 在安卓手机上安装时被提醒为风险软件。该提示会误导用户停止使用 APP，且对品牌官网产生严重质疑，造成一定的客户流失，同时也有损品牌形象。该案例通过沟通处置后，在 3 个自然日后恢复正常下载，无风险提示。

图 66：手机安卓系统误判某品牌官网存在风险

06 中外数字风险场景的相似与差异

数字风险具有很强烈的全球属性。

从企业的角度，公司业务要服务于全球用户，资产必然会暴露在整个互联网之上。从攻击者的角度，他们往往会藏匿于非攻击目标所在的国家来逃避监管制裁，比如以中国企业为欺诈目标的组织或团伙一般会把钓鱼网站搭建在海外。这样一来，即使目标企业发现自己被仿冒或者钓鱼，大多数情况也无能为力，无法及时有效的进行制止或关停。

天际友盟团队常年从事国际数字风险防护实践，为客户的全球化业务保驾护航。基于过去几年的实践总结，我们从如下的几个维度总结了一些中外数字风险防护的差异。

维度	差异	差异说明
攻击目标	金融行业	国外：金融行业钓鱼大多数集中在规模较大的商业银行。从自动化的角度，国外的高级攻击团伙更倾向于网银木马，因此只专注于钓鱼的团伙都属于比较低端的诈骗团伙； 国内：金融行业仍然是钓鱼团伙攻击的主要目标，但由于互联网环境、网银的普及程度、手机银行的发展速度和语言障碍导致了网银木马并没有机会占领国内的主流市场，因此在金融行业，尤其针对银行及证券公司，攻击者更多的还是会依赖各种钓鱼手段盗取身份及敏感信息，同时由于国内网民整体来说网络安全意识不高，使简单的钓鱼攻击很容易达成。
	互联网在线服务平台	国外：互联网头部平台非常聚集，而其他小型平台基本没有规模，所以攻击主要集中在较大的几个交易平台（如 ebay、amazon 等）； 国内：互联网飞速发展，除了几家大型电商交易平台，还包括在线订餐、快递业务等，网上业务已经涵盖了生活的各个方面，因此被攻击的范围比较广。"
传播方式	电子邮件	国外：邮件仍然是主要的商务沟通方式，因此利用钓鱼邮件进行攻击在国外依然是非常主流的传播方式； 国内：随着移动办公的迅速发展，邮件已经不再是主流的沟通工具，即时通信工具和协同办公平台（例如钉钉、企业微信）比邮件沟通效率更高，应用的也更加普遍。但邮件沟通在外贸业务和跨国业务的企业中还是比较常见，反而会成为风险的聚焦点。
	短信	国外：钓鱼攻击其主要传播途径是通过邮件，也有部分通过社交媒体，短信占比不高； 国内：在中国虽然邮件的使用率比较低，但由于手机的普及程度高，通过短信等方式的传播更加广泛，受众面更大，依然非常盛行。
	社交媒体	数字品牌在社交媒体上的风险的不同，主要是侧重的平台不同，比如： 国外数字风险高发的社媒平台： facebook， twitter, Instagram, Linkedin 等； 国内数字风险高发的社媒平台：微博、微信公众号、头条、抖音、小红书、快手等。

传播方式	移动 APP	对于 iOS 系统来说，由于苹果统一的管理，国内外基本只有官方的 APP 商店； 而对安卓系统而言： 国外，对于官方 APP 下载渠道的一般理解就是 google play，其他商店一律被视为第三方商店。 国内，安卓系统并没有一个指定的官方 APP 商店，几乎国内每个大的安卓手机厂商都有自己的 APP 商店，还有各平台推出自己的 APP 商店。但是由于各个商店对 APP 的安全把控程度不一样，对开发者身份的验证和软件的安全性的标准都不相同，这导致了标准参差不齐的现象，使得很多欺诈或者是恶意软件可以从第三方 APP 商店正常下载。"
攻击特点	基础设施	国外：钓鱼攻击的基础设施以肉鸡和免费主机为主，这两种攻击类型，在 10 年前几乎占到国外钓鱼攻击的 90%。近年来逐渐出现了恶意相似域名注册，占比虽然处于上升阶段但并不是主流攻击手段； 国内：大部分钓鱼的攻击，都是以注册相似的恶意域名进行仿冒的。 这两者有很大的区别，攻击者利用恶意域名作为攻击手段，成本比肉鸡和免费主机要高很多，处置难度也较大，这样就可以保证钓鱼攻击过程的持久性，为攻击者争取更多的欺诈时间。
	模板设计	国外：通常针对不同的对象使用不同的模板； 国内：国内企业的团伙经常使用相同的模板进行不同的品牌的攻击，虽然重复性较高，但攻击更有效率，且被阻断或投诉的机率并没有高很多。
发展状态	甲方重视程度	国外：国外企业的品牌保护意识比较强，会主动去打造一个安全的品牌形象，对于数字风险防护的需求一般出于自身对外部威胁、安全防护的压力，有完善的相关法律支撑。 国内：国内企事业单位对于数字风险防护的需求多出自于合规等外部压力，通常是被动的政策有需求、有通报才会有行动，对数字风险重视程度不足。"
	情报共享机制	国外：国外服务提供商共享大量英文情报，侦测主要集中在对数据的分析、剥离和优化。但是国外服务商区域化支撑不成熟，主要是语言能力不足和用户群体的不同，极少能够找到针对中国品牌的风险数据。 国内：情报掌握在少数服务商手中，没有完善的情报共享机制，侦测主要是靠服务商的自主研发的侦测机制，并且只有为数不多的厂商提供数字风险服务进行侦测数据的整合和关停。

07 数据风险防护指南

随着互联网的迅猛发展，数字化转型已成为全社会无法回避的挑战，2020 年席卷全球的新冠疫情更是加速了这一进程。然而，数字化转型的同时也带来了各种各样的数字风险，企业、机构等各类主体的数字资产也面临着更多的外部威胁。

在数字经济时代，各类主体对数字风险防护的需求正与日俱增。组织需要一个标准的、规范化的方法来应对新生的数字风险，以期满足对风险管理的成熟度要求。IDRR 框架是一个基于生命周期的数字风险防护方法论，可以和信息安全框架结合，有效解决上述的问题和挑战。

7.1 数字风险防护框架（IDRR Framework）

IDRR 框架，基于数字风险防护生命周期，分为识别（Identify）、监测（Detect）、响应（Response）、恢复（Recovery）四个阶段。该模型将持续改进融入了数字风险防护模型，可为企业提供数字风险的全生命周期管理。

识别（I）：“识别”是指了解组织运营（包括任务、职能、形象或声誉）、组织资产和个人的网络安全风险，识别和管理企业资产要素及其对业务目标的重要性，并用于支持运营风险决策。具体又可分为四个步骤：

第一，明确有价值的数字资产。成立统一管理的小组，梳理企业有价值的数字资产，企业资产包括但不限于网站、域名、官方 APP、企业社交媒体账号或高管个人社交媒体账号，以及企业内部数据、文件、代码等。

第二，评估数字资产的足迹与暴露面。在资产梳理工作完成后，由专业人员根据网站域名白名单、官方 APP 域名白名单或授权下载渠道白名单、关键字、数字水印、HASH、特定字串等，评估上述数字资产在互联网上的传播路径及暴露面。

第三，数字风险与损失分析。分析企业数字资产可能或已经面临的风险，并预判其对企业业务可能会或已经造成的损失。

第四，制定数字风险防护策略。根据企业所关注的数字资产及面临的风险，制定相应的数字风险防护策略。

监测（D）：“监测”是指对企业的信息、资产、数字足迹进行全面监测，以识别网络安全事件和异常活动，了解事件的潜在影响，评估并反馈事件风险程度。

监测能力有赖于两大体系，一是情报体系，包括 NOD（新观测到的域名）、威胁情报、第三方情报、暗网情报等；二是技术体系，包括爬虫对抗、NLP（自然语言处理）、图像识别、音频识别、视频识别等技术。

监测对象针对两类资产：一是隐藏资产，包括探测扫描、远程控制、恶意邮件、IDS、SIEM/SOC、态势感知等；二是暴露资产，包括域名安全、移动 APP、企业社交媒体账号、高管社交媒体账号、企业数据、代码凭证、搜索引擎等。

响应（R）：“响应”是指执行响应流程和程序，以防止事件扩散、缓解事件影响和消除事件，针对事件活动酌情与内部和外部利益相关方沟通协调，包括寻求执法机构的外部支持。

响应的具体流程为，对数字资产可能面临的钓鱼仿冒、品牌侵权、数据泄露、威胁误报等威胁风险，通过与覆盖

全球的 VPS 提供商、域名注册商、网络提供商、各国各类监管机构、应用商店管理者、社交媒体平台管理者沟通协作，对上述数字风险进行快速关停处置，并对处置结果进行持续跟踪，确保数字风险的彻底根除。

恢复（R）：“恢复”是指与内部和外部各方协调恢复活动，执行和维护恢复流程和程序，以确保及时恢复受网络安全事件影响的系统或资产。吸取经验教训，纳入今后的改进恢复计划和流程。其次，对目标品牌或资产，在互联网上做持续的监测，如出现风险“复活”的情况，能够做到第一时间预警和再处置，做到暴露资产的风险可控及稳定安全。

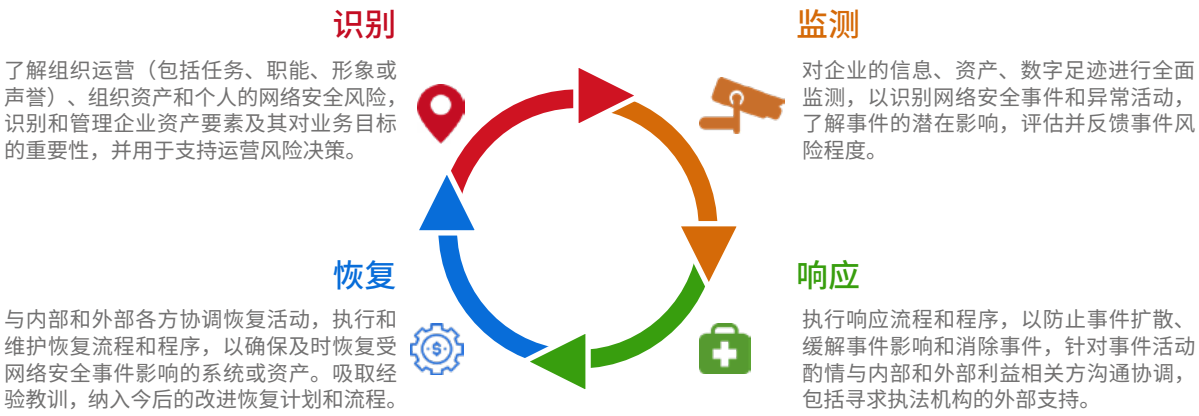


图 67：数字风险的全生命管理周期

7.2 识别数字风险防护需求

随着数字经济的发展，任何行业、任何企业、任何机构，都可能面临各种各样的外部威胁及数字风险。企业、机构等各类主体对数字风险管理的需求正与日俱增。根据我司的观察及调研，金融行业、影视文娱行业、数字资产行业、知识付费行业以及大型国央企、泛政府机构，由于各行业所具有的特殊性，更易遭受不同类型的数字风险的威胁，其需求表现在业务风险和合规风险领域。

7.2.1 金融行业

金融行业，因其业务属性的特殊性，向来是各种仿冒欺诈的重点目标。数字金融欺诈手段表现出专业化、产业化、隐蔽化、场景化等新特征。 根据 APWG 2020 年 4 季度的报告，针对金融机构的钓鱼攻击仍是最普遍的，攻击者仿冒企业真实网站的 URL 地址以及页面内容，试图骗取各类受害用户的银行卡账户、身份账号、各种密码等私密信息。

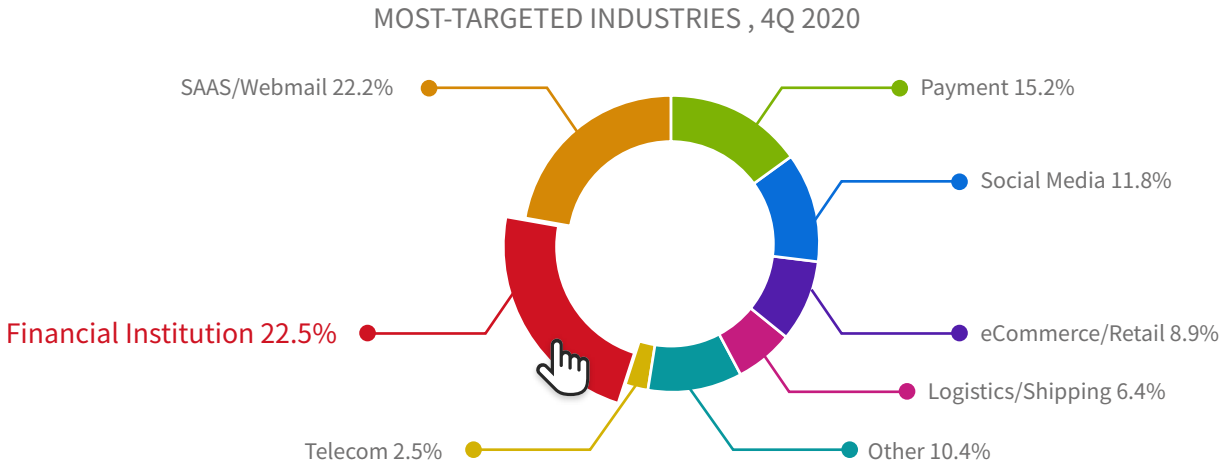


图 68：针对金融机构的钓鱼攻击最为普遍

数字金融欺诈，是一个行业乃至整个社会需要面对的问题。金融监管机构对此有明确规定，金融机构必须加强安全技术防范措施，需加强主动侦测钓鱼网站机制建设，主动搜索钓鱼网站，并采取多种措施及时关闭钓鱼网站，否则将面临被监管通报批评的后果。早在 2011 年，中国银监会就下发《中国银监会办公厅关于进一步加强网上银行风险防控工作的通知》，各银行业金融机构应高度重视网上银行风险管控，加强对仿冒网站等“钓鱼”诈骗事件的防范，与此同时加强反“钓鱼”应急处置机制建设，有效切断“钓鱼”诈骗渠道。2020 年，中国人民银行发布《网上银行系统信息安全通用规范》，该规范中专门规定了“防钓鱼”的要求：

图 69：《网上银行系统信息安全通用规范》

- 金融机构应具有防网络钓鱼的功能
- 应采取防钓鱼网站控件、钓鱼网站监控工具、钓鱼网站发现服务等技术措施，及时监测发现钓鱼网站，并建立钓鱼网站案件报告及快速关闭钓鱼网站的处置机制
- 应加强防钓鱼的应用控制和风险监控措施

疫情期间，群众为了配合防疫要求，购物、办公等日常活动尽量借助网络完成以减少出行。相较于疫情前，数字人民币的使用范围和交易金额也呈递增趋势。另一方面，人们的生活水平直线上升，逐渐有了积蓄，理财意识也随之强烈。无论老年人还是年轻人，对理财产品的热爱也趋于明显。线上银行不仅帮助人们完成交易，也提供了理财平台，因此在人们生活中的使用率逐渐上升。不少犯罪分子正是看重这一点，制造了大量仿冒银行的钓鱼网站和钓鱼 APP，并巧立名目骗取用户的信任，使用户放松警惕，登录假平台并输入了自己的银行卡号或敏感信息，导致最终造成钱财损失。

图 70：仿冒某知名银行的钓鱼网站

图 71：某地方银行的仿冒 APP

金融行业常见的数字风险场景包括：

钓鱼欺诈

品牌侵权

数据泄露

7.2.2 影视文娱行业

近年来，数字版权作品（包括影视、小说、体育、动漫、图片、音乐、游戏等）被盗版的事件层出不穷，且愈演愈烈。企业的数字作品版权遭到非法窃取后，公开在网站、网盘、社交媒体等平台传播，给版权方和发行方带来重大损失。

以影视盗版为例，在影片制作、发行、上映等不同阶段均有可能发生，给制片方、发行方、院线或授权播放平台均带来巨大损失，且严重影响影视行业产业链的商业收益。《流浪地球》导演郭帆曾对相关媒体表示，为了防止盗版，

他们采取了在制作端层层加密的方式，对素材严格管理，并安排三个防盗版团队在影片上映后进行全天候的防盗版监控。然而实际结果表明，盗版依然防不胜防。该片制片人龚格尔在接受媒体采访时曾表示，“我们估算全部春节档影片到现在为止，网络盗版观看数量超过 2000 万次。这是非常保守的，因为点对点下载无法统计。”按照猫眼提供的平均票价 46 元一张计算，盗版影视造成单票房损失逾 9 亿元人民币。据估计，2019 春节档，因盗版引起的总票房损失高达 15.2 亿。

图 72：电影《流浪地球》

影视盗版在影片制作、发行和播映的任何环节都有可能发生。大部分盗版团队，会通过海外网站、微博、公众号、网盘等多种平台进行交叉传播。这种贯通上下游的技术与分发相结合的模式，使盗版组织自身能够高效运作，同时给制片方带来重大经济损失。

盗版团伙技术进步，隐蔽度高，盗版资源全球散播，形态多样，关停复杂。传统技术屏蔽手法，往往掩耳盗铃，未实际解决问题。传统的法律手段，针对大型网站有一定效果，但对海外小型网站往往束手无策。无论盗版团伙前期如何破解加密、提取码流或非法拷贝，中期如何经过微信、微博、二手交易平台等多平台辗转传播，终极目标都是为了获取商业利益。

文化版权行业常见的数字风险场景包括：

版权盗版

品牌侵权

明星名人仿冒

7.2.3 数字资产行业

当下，全球数字经济发展正处于高速推进阶段。根据前瞻产业研究院 2021 年发布的《中国数字经济行业市场前瞻与投资规划分析报告》，数字经济占全球 GDP 比例有望超过 60%。据 IDC 预测，到 2023 年数字经济产值将占到全球 GDP 的 62%，全球将进入数字经济时代。

随着数字经济的发展推进，数字资产正逐步展现出它的生命力，成为经济金融领域最为活跃的资产形态之一，正受到包括政府、市场机构在内的多方主体的高度重视。数字资产在经济金融市场的价值也日益突出。

2021 年是数字资产市场发展的关键之年。一方面，加密数字资产迎来了爆发式增长。2021 年也是法定数字货币研发进程的关键转折点，多个国家和地区的法定数字货币研发进程提速。其中，数字人民币表现突出，目前处于全球领先地位。截至 2021 年 3 月 18 日，数字人民币已在深圳、苏州、北京、成都等地先后进行了七轮红包试点，共发放数字人民币 1.5 亿元。

正因为数字资产行业的特殊性，相关主体很容易遭到各类型针对性的攻击与欺诈，其精心打造的品牌可能会在瞬间被摧毁。因此该行业对数字风险防护的需求愈发迫切。根据我司观察，从未有一个行业，会遭受到如此多类型的品牌攻击，而攻击方的技术手法之复杂和隐蔽、遭受攻击时的时间敏感性、技术对抗与复活尝试的持续性和在同行业内

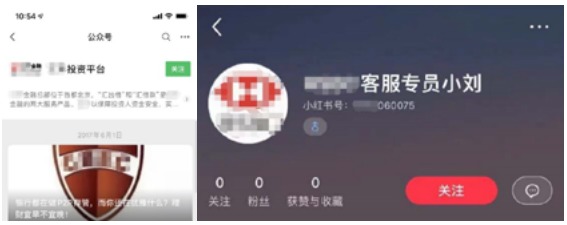


图 73：某银行的社交媒体钓鱼欺诈风险示例

换目标迁徙不断攻击，都是比较罕见的。举例来说，不法分子会通过仿冒目标公司的微信公众号或伪装成该公司的客服，以对潜在用户开展钓鱼欺诈活动，最终使相关用户遭受经济损失。

数字资产行业常见的数字风险场景包括：

钓鱼欺诈

品牌侵权

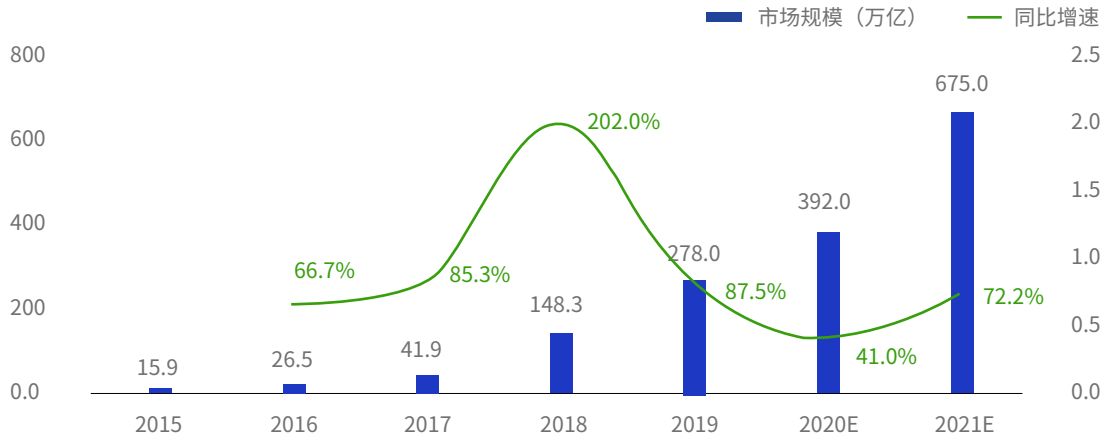
数据泄露

搜索引擎恶意排名

威胁误报

7.2.4 知识付费行业

随着互联网的发展以及移动互联网的兴起，中国知识付费行业迎来了快速发展的阶段。例如，遵循专家模式的知乎，使用意见领袖形式的豆瓣，以及健身、绘画、艺术等各个细分领域细分的公开课、交流社区和专业教学 App 等。受疫情影响的 2020 年，见证了知识付费行业的爆发式增长。中投产业研究院发布的《2020-2024 年中国知识付费行业深度调研及投资前景预测报告》显示，2020 年中国知识付费市场规模达到 392 亿元，预计 2021 年将突破 675 亿元。



数据来源：艾媒咨询

图表 40：2015-2021 年中国知识付费市场规模及预测

与此同时，知识付费也成为了网络著作权侵权的重灾区。以网课为例，不法分子通过录屏、技术破解等形式，使各公司网课资源被黑灰产分子搬运到电商、二手交易平台、社交群组兜售，对版权拥有者造成巨大损失。

网络环境下，知识产权问题的复杂性与特殊性使其保护工作面临新的挑战。尽管《著作权法》、《信息网络传播权保护条例》等知识产权法律法规以及刑法、诉讼法等已进行修改完善，但网络环境下的著作权侵权案件，其作案手段往往具有不低的技术门槛。跨国跨区域作案多，盈利手段隐蔽，侵犯对象也具有市场选择性。这在客观上造成证据分散，使得权利人或公安机关在办理案件的过程中，很难在第一时间提取必要的、关键的电子数据。

知识付费行业常见的数字风险场景包括：

品牌侵权

数据泄露

搜索引擎恶意排名

7.2.5 大型国央企业

过去几年间，大规模数据泄露事件层出不穷，社会各界对于数据资产安全的关注度与日俱增。2020 年的新冠疫情席卷全球，更是使得网络威胁形势日趋严峻。

随着大型国央企的信息化程度不断加深，数据已然成为组织的核心资产。掌握国家经济命脉的国央企在充分享受信息技术这把“达摩克利斯之剑”带来的红利的同时，也面临数据泄露风险，特别是利用云计算、大数据构建的数据高度集中的信息基础设施，其脆弱性带来的风险不容忽视。企业产品信息、市场战略、技术发明等核心内部资料一旦遭泄露，不仅会直接导致企业利益受损，还可能引发重大的安全问题，造成严重的品牌负面影响。同时，个人信息数据也是企业的核心资产之一，企业在强调权利的同时，也具有责任和义务来保护用户的隐私数据。

图 75：某大型国家能源企业的仿冒网站宣传非法赌博示例

习总书记在 2014 年就提出了“没有网络安全就没有国家安全”的指导思想。为适应日益严峻的网络安全形势，各个国家持续加大力度对数据进行保护。我国先后出台了《国家网络空间安全战略》、《网络安全法》等政策法规，《数据安全法》、《个人信息保护法》等法律也在加紧制定中。这些法律法规督促全社会，特别是国企、央企，加强网络安全建设，保护企业核心数据资产，健全管理机制，提高安全意识，采取有效措施降低敏感信息泄漏概率，提高企业核心竞争力。

大型国央企常见的数字风险场景包括：

品牌侵权

数据泄露

7.2.6 泛政府机构

泛政府机构包括公安、税务、教育、医疗等。这些政府机构及大学等教育机构具有一定的权威性，易获得一般公众的信任。因此针对此类主体的网页篡改、侵权事件频发，例如：某网站假冒政府网站，盗用政府网站名称，违规发布大量虚假信息，误导网民，造成不良社会影响；某网站仿冒政法网站，违规提供虚假证书查询和个人信息收集，侵犯公民合法权益；还有些仿冒网站会出现色情、赌博信息或转链非法网站等。以上行为均违反了《中华人民共和国网络安全法》、《互联网信息服务管理办法》等规定，严重干扰网上信息传播秩序，损害政府部门、高校等机构的形象及公信力，危害群众利益。

图 76：某省税务局的仿冒网站示例

2018 年，工业和信息化部印发《关于纵深推进防范打击通讯信息诈骗工作的通知》，其中重要任务之一即加强钓鱼网站和恶意程序整治，有效降低网络诈骗威胁风险，加强对仿冒政府、教育、金融机构等钓鱼网站和涉嫌诈骗类恶意程序的监测分析和信息共享，及时依法处置钓鱼网站和诈骗类恶意程序，及时提醒诈骗类钓鱼网站和恶意程序风险情况。

根据国家互联网应急中心（CNCERT）监测数据，2020 年 CNCERT 共检测发现我国境内被篡改政府网站 1030 个，较 2019 年同期（787 个）增长 30.9%。

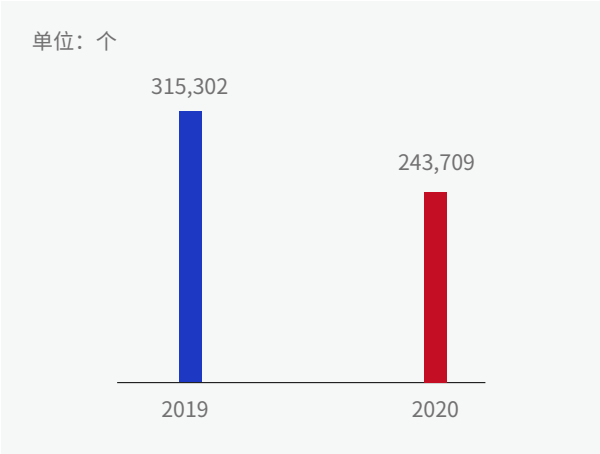


图 77：我国境内被篡改网站数量

泛政府机构常见的数字风险场景：

品牌侵权

数据泄露

7.2.7 高等教育行业

每年伴随全国高校招生工作的陆续启动，一些不法分子开始把高等院校作为新的钓鱼网站仿冒对象。待高校招生咨询和录取工作将全面展开之时，预计届时以高等院校、分数查询、志愿填报、出国留学等教育类网站可能成为犯罪分子实施网络钓鱼瞄准的重点对象。据中国反钓鱼网站联盟秘书处相关负责人表示，根据往年教育类钓鱼网站特点来看，常见的诈骗手段可能有三种：其一、制作以正规高校网站、在线填报志愿系统等为仿冒对象钓鱼网站；其二，制作传播以骗取敏感信息为目的的钓鱼网站；其三，制作发布“山寨高校”网站。

曾被媒体披露的“广州理工学院”、“华北师范学院”等“山寨高校”，擅自盗用其他正规高校网站上的教师头像和简介，胡乱拼凑而成的“招生简章”上竟然大胆印着克隆版的校徽，这样的资料真真假假的山寨网站让学生和家长根本难以区分。同时，该负责人表示，正规高等院校网站不太重视建立健全的假冒钓鱼网站机制，很容易被不法分子利用，这不仅严重损害了家长和学生的利益，还无形中破坏了正规高校的形象，也严重扰乱了互联网教育界的秩序。

除了上述的虚假招生，仿冒高等院校的钓鱼网站还常用于为非法活动进行引流。很多仿冒网站表面上大致与校方官网无异，但实质在某一版面上宣传着涉黄涉赌或其他不法活动的广告。不明就里的网友可能就会被误导到非法网站上而造成钱财或敏感信息的泄露。这一行为严重影响了高等院校的声誉，也破坏了中国教育行业在网民心中的正面形象。

图 78：国内某知名学府的足彩钓鱼网站

随着经济水平的提高，越来越多的家庭选择送孩子出国留学，美国、英国、加拿大、澳大利亚等等都是大家的热门选择。2021 年 4 月央视财经报道，本年本硕博出国留学申请人数激增 50%，创历年新高。正是这样庞大的潜在市场，大量国际犯罪分子也将黑手伸向留学生群体。

虽然现如今信息技术日益发达，我们能够更容易地接触到国外大学更准确的资讯，但是获取到的信息是片段式的，且掺杂着真真假假。对于不是很了解留学申请的学生，尤其是英文使用不太习惯的家长来说，想要辨认并筛选出真正对自己有利的信息，实在太难。在这样的大环境下，很多不法分子看到了自己的“商机”。他们会制作各类仿冒国外官网的钓鱼网站，通过某些特定手段来骗取钱财或敏感信息。

BBC 就曾曝光过英国某大学官网被不法分子仿冒，并发邮件给留学生，专门骗取其学费的案例。该钓鱼网站的诈骗套路主要有两种，第一种是在学生注册，以及申请远距离课程的时候，直接收费。第二种则是收集学生们的申请资料，比如：护照号码、手机号码、全名、出生日期，信用卡信息等等，用于后续诈骗。值得注意的是，无论是哪种，一旦中招，追回损失的可能性都很低。

图 79：英国某知名学府的钓鱼网站

该案例被媒体曝光后，虽然涉事学府已在社交媒体上澄清与钓鱼网站的关系，但单一事件的处置很难保证其他大学没有类似的钓鱼网站。为了防止合法权益被损害，留学生们不仅要提高防范意识，各大学也有必要对损害自身声誉的侵权网站进行监测。

高等教育行业常见的数字风险场景：

品牌侵权

数据泄露

7.2.8 外资机构

自中国改革开放以来，外资企业的投资规模从小到大、水平由低到高、区域从沿海到内地。在中国波澜壮阔的繁荣进程中，外商投资企业始终是重要的参与者、见证者、和受益者，并且中国未来仍是跨国公司投资的理想目的地。截止 2021 年，外资企业在我国已涉足金融、证券、保险、餐饮、酒店、零售、物流、电子商务、服务、投资等各行各业。虽然外企数量繁多、种类错综复杂，但在数字风险来临之际，大多经历着同一困境。

外企入驻中国市场的大多是享誉世界的国际知名品牌，通常已树立了良好的品牌形象，赢得了消费者的认可。犯罪分子正是看重并利用其对消费者所产生的影响力，大量制造仿冒外资品牌的钓鱼网站来对网民进行钱财和敏感信息的欺诈。不少群众出于对品牌方的信任而放松警惕，进而被诈骗者钻了空子。

此外，即使发生了钓鱼或侵权行为，外资企业由于不熟悉我国法律法规，无法及时对风险作出响应而导致错过最佳解决时间，期间还可能会导致更多网民的伤害。

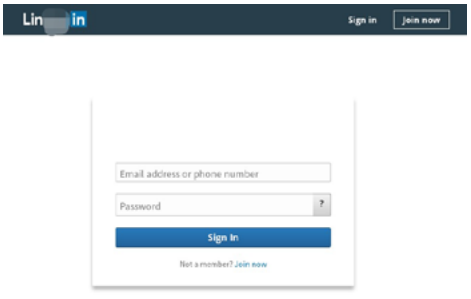


图 80：美国某知名社交媒体的钓鱼网站

图 81：美国某大型物流公司的钓鱼网站

外资企业常见的数字风险场景：

钓鱼欺诈

品牌侵权

数据泄露

7.2.9 医疗卫生机构

随着 5G 时代的到来，个性化医疗、远程诊断、远程治疗等逐渐走进百姓生活。而这一切都以体量庞大的健康医疗大数据信息为基础，健康医疗大数据已成为国家基础性战略资源。我国深刻认识到健康医疗大数据的重要性，并从国家层面推动健康医疗大数据的应用，以抢占创新医学研究、精准诊断、个性化健康管理和移动医疗等前沿阵地。然而，随着医疗大数据规模日益庞大，这些数据的安全问题也日益凸显。越来越多的数据被公开贩卖，被犯罪者利用。医疗行业关系国计民生，医疗数据一旦遭到篡改、破坏和泄露，势必对医疗机构的声誉、医患双方的隐私及健康安全构成严重威胁，甚至影响社会的和谐稳定。

根据 IBM 发布的《2021 年数据泄露成本报告》显示，2021 年全球医疗数据泄露平均成本高达 923 万美元，增幅为 29.5%，医疗保健行业的数据泄露成本连续 11 年位居首位。医疗保健行业在 2020 年已确认的数据泄露事件同比增加了 58%；2018 年至 2020 年中，超过 93% 的医疗保健组织出现过数据泄露。可见，医疗行业深受数据泄露的毒害。

图 82：疫情期间胶州某医院泄露患者及家属的就医记录

除了数据泄露，针对医疗行业的钓鱼行为也是屡见不鲜。某疫苗生产公司因生产新冠疫苗而成为网络钓鱼攻击者的热门假冒对象。近日，根据 INKY 的一份最新报告，2021 年 8 月 15 日左右开始的一个网络钓鱼电子邮件活动冒充了该公司，试图从受害者那里窃取商业和财务信息。犯罪者购买了多个匿名的仿冒企业官方网站的域名，并注册了电子邮箱，给收件人发送了涉及紧急报价、招标和工业设备供应等主题的邮件以诈骗机密商业信息。

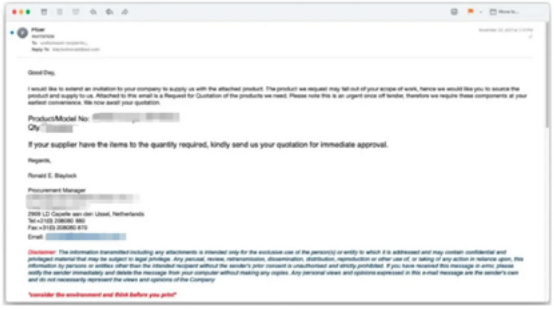


图 83：仿冒某疫苗生产公司的钓鱼邮件

医疗卫生机构常见的数字风险场景：

数据泄露

钓鱼欺诈

品牌侵权

7.2.10 互联网行业

近几年，互联网行业在我国发展如火如荼，带动经济发展的同时也有效带动我国产业结构的升级。不仅有阿里、腾讯、美团这样的龙头企业为数字化科技创新做出贡献，同时也孕育了一批中小型互联网企业来扩大产业规模。如今，这些互联网企业已深入到百姓生活的衣食住行，为人们提供最优质的服务。

从社交媒体到零售，各类互联网品牌正在借助越来越多的触达点来与消费者进行互动。消费者在触达点的安全感受程度会成为商业差异的重要来源，这些触达点的安全性保障了消费者与品牌互动时每一步的基本安全。因此，互联网企业对数字风险防护的需求正与日俱增。

互联网企业保护其数字资产的难点来源于其数字资产的体量庞大，与百姓的生活关系紧密，所面临的数字风险类型又纷繁复杂，且内部安全团队规模有限，仅靠人工搜索进行品牌维护所能达到的效果微乎其微。另一方面，数字风险还会随着时间推移而产生变化来逃避监测。这些都让安全人员在应对过程中精疲力尽。

针对互联网企业的数字风险种类很多，但主要集中于网站钓鱼仿冒、品牌侵权和 APP 仿冒这三类。

图 84：某知名互联网企业 APP 在第三方应用商店未经授权上架

图 85：某知名互联网企业的钓鱼网站

图 86：某知名互联网企业的商标侵权网站

互联网企业常见的数字风险场景：

网站钓鱼欺诈

品牌侵权

AP 社交媒体仿冒

数据泄露

7.2.11 游戏行业

近年来，电子游戏经济作为一种娱乐消费品，随着日益强大的网络经济，现在已是娱乐产业中相当重要的组成部分。Newzoo 预测，2021 年游戏行业的总收入为 1758 亿美元，略低于 2020 年的总收入，但仍显著高于新冠肺炎疫情爆发前的数字。虚拟世界之所以收到网民的欢迎，主要由于游戏不仅提供放松的机会，还被赋予了与陌生人进行社交活动的属性。目前全球拥有 27 亿游戏玩家，手机游戏尤其吸引了越来越多的用户。这种快速增长很大程度上归功于移动游戏的激增以及新冠肺炎疫情大流行期间对社交互动的关注。

但正当游戏行业蓬勃发展之时，2021 年 8 月卡巴斯基发布了《2020-2021 游戏相关网络威胁情报报告》。报告表示针对 PC 和手机玩家的攻击也在随着游戏行业的收入快速增长。从 2020 年 7 月 1 日到 2021 年 6 月 30 日，遭遇与游戏相关的恶意软件和流氓软件（或者不需要的软件）的用户总数为 303,827。其中，共有 50,644 名用户试图下载 10,488 个伪装成十大受欢迎手机游戏的恶意钓鱼 APP，共被检测到 332,570 次。

此外，存在威胁的手机游戏中 83% 是由于 APP 植入了广告软件，累计影响 48,492 名用户。虽然广告软件并非恶意，

但非法广告会降低用户体验的质量并使用户数据处于危险之中。此外，由于具有高度侵入性，广告软件经常使移动设备无法使用。类似 APP 可能存在在第三方应用商店未经授权上架的可能，且应用商店未对 APP 进行技术检测。

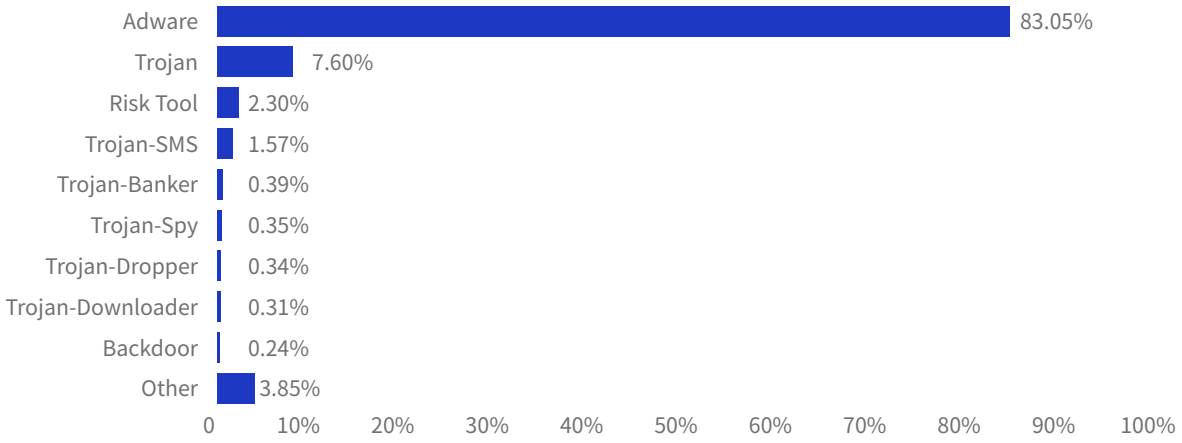


图 87：游戏 APP 存在威胁类型

除了广告软件，调研也监测到不少危险的恶意软件，例如个人信息和银行账号窃取工具，通常会导致用户丢失账户凭据、损失金钱（包括加密货币）。

网络游戏行业常见的数字风险场景：

APP 仿冒

钓鱼欺诈

数据泄露

品牌侵权

7.3 数字风险意识管理

如同网络安全风险意识是网络安全的重要部分，数字风险意识决定了企业管理数字风险的态度，是数字风险防护的源头。市场、法务、风控、人力资源、财务、高管、技术团队等等，都可能是数字风险的潜在目标。因此培养内部人员的风险意识，是数字风险防护体系中不可缺少的一环。数字风险意识管理，可以从以下方面着手：

7.3.1 落实管理机构

在数字风险防护工作中，首要任务是成立专门的团队，团体成员应来自包括 IT、法律、财务、业务在内的多个部门。团队应明确数字风险防护的策略、规范，落实相关责任，保证工作能够长期持续的得以执行。

7.3.2 在线宣传教育

利用企业网站、APP、公众号等途径，进行网络安全文化宣传及普法宣传。同时，通过课程学习、自测考试、游戏竞赛、主动推送等方式，对内部员工进行在线教育，提升员工的安全保密意识。

7.3.3 专业讲师培训

由专业的培训讲师，举办现场讲座，组织网络安全方面的知识学习，向内部员工讲解、展示、演示各种社工攻击或窃密手段，提升人员的网络安全意识。

7.4 建立完备的数字风险防护机制

根据 IDRR 框架，企业可以建立起完备的数字风险防护机制，包括：

7.4.1 识别数字资产（I 阶段）

明确有价值的数字资产，对数字资产足迹及暴露面进行评估，并对可能的数字风险及损失进行分析，制定针对性的防护策略。企业的数字资产包括但不限于官方域名、移动 APP、社交媒体账户、企业数据、版权文件、核心代码、搜索引擎排名。

7.4.2 实时监测风险（D 阶段）

针对品牌或目标资产，在互联网上实现持续性监测，以识别网络安全事件和异常活动，评估事件风险程度，以确保监测范围的全面性、监测结果的快速性及精准度。

7.4.3 多种方式告警（R1 阶段）

对于已发现的风险事件，具有邮件、短信、微信、电话等多种告警方式，确保责任人第一时间知悉风险情况，以便及时执行响应机制，消除事件影响，防止事件影响的扩散。

7.4.4 快速关停处置（R1 阶段）

对已确认的数字资产面临的各类风险，无论风险事件发生在境内或境外，均可实现快速关停处置，缓解或消除事件影响。同时，具备充分的维权依据、完整的授权链条，以确保处置操作本身的合法合规。

7.4.5 持续跟踪监控（R2 阶段）

欺诈或侵权团伙在遭到打击后，也会调整策略，做持续性对抗。对已处置的数字风险，可进行持续跟踪监控，如出现风险“复活”的情况，可以立即重启响应机制，确保风险的彻底消除。

7.4.6 深度风险分析（R2 阶段）

对于已监测的数据，可以进行数据汇总，并生成深度分析报告，吸取其中经验教训，将之纳入今后的改进恢复计划。主动发现、积极防御，将数字风险防护融入到日常工作流程中。

7.5 数字风险防护外包服务评估

由于数字风险主要分布在企业可防护范围外部，对防护的各阶段都提出了技术、管理上的挑战。为了降低数字风险应对成本，企业通常采用外部服务商的方法应对数字风险，因此，针对外部服务商的评估也甚为关键，通常针对外部服务商可以采取以下综合因素进行考量：

7.5.1 覆盖全球

成熟的外部服务商需通过威胁情报交换、新注册域名监控、DNS 请求监测以及主动探测等技术，建立一套覆盖全球的数字风险监测系统。钓鱼仿冒与侵权对象全球分布，成熟的外部服务商可与覆盖全球的网络服务商沟通合作，无论恶意目标主体在境内或境外，均可实现快速关停处置。

7.5.2 场景全面

针对客户的不同业务场景的需求，成熟的外部服务商的服务范围可覆盖各类网络平台，诸如 Web 网站、App 商店、社交媒体、网盘存储、知识社区、深网 & 暗网等。具有全面的数字风险场景，包括但不限于钓鱼欺诈、品牌侵权、数据泄露、版权盗版、威胁误报、搜索引擎恶意排名等。

7.5.3 策略成熟

成熟的外部服务商拥有体系化的应对策略。可运用机器学习、自然语义处理、数据挖掘等深入分析技术，为用户提供持续性的风险溯源追踪。具备多语种沟通能力。熟悉不同平台的处置流程。链接全球各地法律服务体系。

7.5.4 处置快速

数字风险事件发生时，往往有极高的时间敏感性，成熟的外部服务商需要在最短时间内做出响应，消除各类风险，恢复品牌声誉、保护商业价值，其对各类风险的处置时长保持世界同行业的领先水平。

7.5.5 服务效果

成熟的外部服务商可为全国各地的客户提供及时、高效、优质的服务。可实现 7*24 小时实时监测并响应，通过邮件、短信、微信等多种方式向客户告警。具有全球覆盖的处置能力，在证据充足的前提下，关停成功率超过 95%，有标准的交付 SLA 规范。可提供深度风险分析报告，帮助客户完善应急响应机制。

7.6 中国企业国际化进程的数字风险挑战

7.6.1 跨境对抗

对于针对中国企及其用户群体的数字风险，不法分子往往将服务器部署在海外区域，为了逃避监管和打击，往往服务器等资源部署在海外区域，以逃避监测、逃避监管、逃避打击，这就使数字风险的发现及消除增加了实施难度。

7.6.2 时间敏感

数字风险发生时往往很紧急，具有极高的时间敏感性。一旦错过解决问题的最佳时间，企业的损失非但不能得到及时挽回，反而会进一步扩大。

其次，对于网络攻击行为而言，其托管主体的转移速度很快，很难用传统手段去反击。

7.6.3 语言障碍

由于数字风险遍布全球各地，风险处置工作需要企业与全球各类服务商、各大社交媒体平台、监管机构等进行沟通。这对于企业而言，需要付出极高的时间和精力成本。

7.6.4 出海护航

随着国内企业能力和水平的不断提高，有“走出去”需求的企业越来越多，而这些企业在“走出去”过程中则可能面临各类海外的数字风险。但是大部分企业不熟悉国外的语言环境，在识别自身风险阶段就已踟蹰不前，更不用说开展风险的处置工作。

7.7 跨国公司落地的数字风险挑战

7.7.1 中文语境

外国企业进入中国市场后，因自身品牌知名度，也可能面临各类数字风险，但是大部分企业不熟悉中文的语言环境，以及中国国内的产业形态的快速变化，给外国企业识别自身风险带来极大困难。

7.7.2 不同法系

不同国家和地区的法律通常存在较大差异。外国品牌在国内落地后，往往因为不熟悉中国的法律体系规范，不适应中国的法律生态，在遭遇数字风险后，无法采取正确的维权措施，这严重阻碍其业务推广和品牌建设工作。

7.7.3 应对策略

外国企业面对发生在中国境内的数字风险，通常缺乏成熟且体系化的应对策略。国内主流服务商、社交媒体平台的判定规则各不相同，国内公司与国外公司的工作习惯也存在较大差异，导致沟通低效、处置时间长、处置成功率低的问题。

08 总结

网络时代下，越来越多的机构、企业、个人意识到数字风险防护的重要性，也越来越重视维护自身的数字资产及品牌形象，以及背后隐藏的价值。

但是本文所提及的数字风险缘起于其公开性，因此防护工作存在诸多难点问题，只能从事件发生展开响应。许多企业缺乏经验，遇到问题时，往往陷入手足无措的窘境，延误甚至错过解决问题的最佳时间。

天际友盟建议采用 IDRR 模型，以合规需求和业务需求作为数字资产风险梳理的切入点，建立完备的应急响应机制，同时做好员工的安全意识培训、甄选数字风险合作伙伴，将数字风险防护融入到日常工作流程中。

天际友盟

TianJi Partners

你身边的数字风险防护专家

400-081-0700 www.tj-un.com

市场合作：mkt@tj-un.com 客户服务：service@tj-un.com 合作伙伴：partner@tj-un.com