CSC

2025年度
知识产权前沿报告
主动防范知识产权侵权

引言：瞬息万变、风险重重的世界

企业的声誉与其在线形象息息相关。这让知名品牌成为不法分子觊觎的目标，他们通过建立欺骗性网站、仿冒产品或标识、创建虚假的社交媒体账号等手段实施诈骗。

仿冒作假的门槛大幅降低，知识产权（IP）侵权变得空前容易。侵权行为的识别和追究难度也日益增加，仅凭勒令停止侵权的通知函，往往不能让侵权者就此收手。

为应对这些挑战，企业宜采取一系列策略来加强知识产权维权，保护自身的商标权、版权和其他知识产权。

在法务团队资源日益紧张的当下，企业应如何与营销、IT 和安全团队更紧密地合作，优化知识产权保护工作，并确保预算用在刀刃上？

“诈骗分子实施知识产权侵权的能力正以惊人的速度进化，因此，提高对当前态势的认知、对技术的注重程度，并加强域名相关团队之间的协作，对各方都大有裨益。”CSC 首席法务官 Ian McConnel 表示，“我们必须认识到，域名管理是网络安全战略的关键组成部分，绝不仅限于保护几个核心域名。”

我们的专家

Ian McConnel
CSC 首席法务官

Ihab Shraim
CSC 数字品牌服务部首席技术官

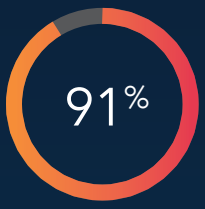
Elliott Champion
CSC 品牌保护和反欺诈全球产品总监

Mary Jo Murphy
CSC 品牌和欺诈服务产品经理

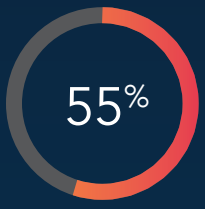
研究的主要发现

2025年第二季度，我们对300位资深法律专业人士做了调研，发现如下：

线上知识产权侵权发生率正在上升，预计还将持续增长



绝大多数（91%）受访者对线上知识产权侵权的威胁表示担忧。



超过半数（55%）的受访者预计未来三年线上知识产权侵权将显著增加。

受访者列出了他们曾遇到过的线上知识产权侵权类型，排名前三的如下：

假冒伪劣

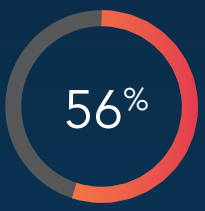
商标滥用

假冒身份

知识产权侵权日益增多，人工智能（AI）在其中扮演重要角色

大多数（88%）受访者表示，搭载 AI 的系统正推动着侵权频率的增加。

受访者认识到外包线上知识产权侵权监控的益处



超过半数（56%）的受访者表示，他们已将部分线上知识产权侵权监控业务外包出去，而且正在积极考虑外包更多业务。

大多数法务团队已与 IT 和安全团队合作，以详细了解知识产权侵权风险

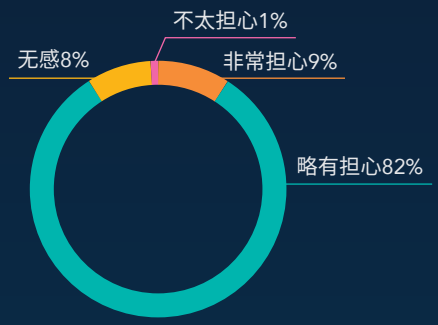
近三分之二（64%）的受访者将他们与 IT 和安全同事的合作紧密度评为“强”（在五分为最高的评分标准上，他们给出了四分），**另有22%**的受访者表示他们与 IT 和安全团队的合作极为紧密。

知识产权侵权发生率持续上升

过去几年，在多种催化因素的共同推动下，知识产权侵权领域发生了深刻变化。

这些驱动因素多种多样，包括犯罪软件即服务（CaaS）工具包的兴起、生活成本的持续上涨以及持续增长的网购。所有这些都在助长知识产权侵权行为，进而损害公司的声誉和利润。

值得注意的是，在 CSC 的全球调查中，超过90%的受访者表示，他们担心线上知识产权侵权会对像他们这样的企业构成威胁。



四分之一的受访者表示，过去12个月，其所在企业面临的线上知识产权侵权“显著”增加；约三分之一（35%）的受访者表示，过去三年，其所在企业面临的线上知识产权侵权“显著”增加。

据受访者报告，最常被利用的三大资产为：

- 互联网内容或品牌内容（45%）
- 移动应用（30%）
- 线上市场（17%）

CSC 品牌和欺诈服务产品经理 Mary Jo Murphy 表示：“人们总是在寻找更便宜的产品，例如，药品、汽车零部件和消费品，这正给了诈骗分子可乘之机。”

展望未来，大多数（89%）受访者预计未来三年知识产权侵权将会增加。九成（90%）受访者预计未来12个月知识产权侵权将会增加。

贵司最担心以下哪些类型的线上知识产权侵权？

- 假冒伪劣
- 商标滥用
- 假冒身份
- 设计权滥用
- 版权滥用

“如何看待这些类型的侵权行为取决于您的视角，”Ian 补充道，“如果我是一家面向消费者的公司，我最担心的就是假冒伪劣商品；但如果我是一家金融服务公司，我更担心的是诈骗分子盗用商标，对客户实施网络钓鱼或网络攻击。”

> 在线形象同样代表着您的声誉，这意味着您必须以不同于以往的方式守护您的声誉。针对企业的威胁层出不穷，而域名和知识产权是最容易被攻击的目标。过去，诈骗分子会发送成千上万封钓鱼邮件，寄希望于其中2%或3%的人会上当受骗；而如今，诈骗活动更具针对性，成功率也高得多。
>
> **——Ihab Shraim，CSC 数字品牌服务部首席技术官**

打击知识产权盗窃，需筑牢域名保护防线

CSC 品牌保护和反欺诈全球产品总监 Elliott Champion 指出：“域名是人们日常互动与交流的核心要素。它在不知不觉中渗透进生活的方方面面，人们甚至意识不到自己在与域名互动，并想当然地认为自己不会受到侵害。然而，虚假网站域名往往是知识产权侵权的重灾区，诈骗分子从未像现在这样，能够随心所欲、轻而易举地注册任何域名。”

“不知您是否注意到，现在有些餐厅可以使用二维码点餐？当您扫描二维码后，页面会直接跳转至某个域名，而您事先根本不知道会跳转到哪里，全凭信任。”Elliot 解释道，“域名对于日常数字体验的重要性可见一斑。我们都信任域名并与之互动，即便注册一个虚假域名不过几分钟的事。这意味着此类欺诈活动的门槛已经低得令人难以置信。”

应对知识产权侵权，AI 的作用日益凸显

AI 以前所未有的速度融入各行各业，成为全球商业和生产力讨论的核心议题。但另一方面，从欺诈和风险的角度来看，AI 也被用来仿制高度逼真且复杂的知识产权资产，例如，商标、图片和企业内容。随着 AI 及其应用不断加速发展，法务团队深切关注的是，如何最有效地识别风险并防范于未然。

不出所料，在我们的调查中，约九成（88%）受访者表示搭载 AI 的系统正推动着侵权频率的增加。

此外，大多数（93%）受访者表示，他们担心利用 AI 仿造虚假资产的能力可能会对他们的业务产生重大影响。

“如今，利用 AI 生成虚假材料简直不费吹灰之力，而且这些材料极易被恶意利用。”Ian 说道，“需要坐在电脑前，靠敲代码来制作大量虚假网页的日子已经一去不复返。工具在日益精进，这将给技术水平不高的不法分子提供更多作案机会。唯一能限制欺诈者的，就是他们的想象力。”

企业正面临着 AI 带来的新挑战，而且这些挑战还处于不断演变之中。九成受访者表示，他们担心 AI 工具可能使用其企业的数据或知识产权来训练模型，从而生成可被竞争对手利用的内容。然而，大多数有此担忧的受访者认为，他们已采取了充分的保护措施。

一个积极的信号是，许多企业已意识到 AI 的威胁日益加剧，正通过内部培训计划和其他举措来加强防御。

近70%的受访者认为，其企业针对使用 AI 创建知识产权资产所制定的内部指南或政策质量“良好”，另有20%的受访者认为相关指南或政策质量“优秀”。

展望未来，在企业防范 AI 引发的风险方面，培训可能会发挥越来越重要的作用。

区分真假愈发困难

在知识产权侵权方面，受访者最担忧的三大问题之一是身份仿冒，包括利用 AI 生成逼真的高管肖像，以此向员工索要资金。

Ian 表示：“网上有很多关于首席执行官的资料，包括演讲、帖子和视频，诈骗分子可以利用这些素材，在几个小时内创建 AI 替身，足以骗过企业内的许多人。总有一天，我们会看到某个我们日常接触之人的网络替身，它与本人一模一样，让我们无法区分真假。

所幸还没到这一步，当下我们依然能看出虚假视频聊天的漏洞，但这项技术的迭代速度极快，进化速度更是呈指数级增长，说实话，这只是时间问题。

这意味着企业需要建立相应的流程和系统，不能仅依靠个人来辨别通信的真伪，无论通信手段是电话、视频还是电子邮件。只消五年时间，再也没有培训能够有效阻止这些欺诈者。

反击的第一步是关停可能发起此类通信的域名，并部署正确的协议来验证非法通信的来源。”

预算不断增长，但资金却不一定跟得上

在风险和催化因素数量不断增加、类型不断翻新的当下，企业如何调整 IT 专项预算以应对挑战？

我们的研究发现，知识产权侵权和品牌保护方面的预算不断增加：约三分之二（67%）的受访者表示，他们预计未来三年这些预算将“显著”增长，而略低于半数（46%）的受访者预测未来一年预算将出现“显著”增长。

受访者预计未来12月以下领域将获得更多投资：

72%	69%	68%
内部技术	扩大知识产权管理团队人员规模	扩大法务部门人员规模

近半数（44%）受访者预计，企业会加大知识产权业务外包力度，与类似 CSC 这样的专业第三方公司合作。

这些不断增长的投资凸显了一个重要问题：应将资源投入到哪些方面，才能带来最大影响？企业不应试图覆盖所有潜在渠道或域名变体，而应优先将资金用于能发挥最大效用的地方。

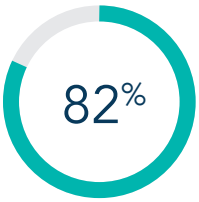
“这不仅仅是增加预算的问题，更重要的是如何使用这些预算。”Ian 表示，“为了跟上 AI 时代的步伐，应对与之相关的问题，你们投入了多少资金？为了配置合适的资源，适当降低风险，你们又投入了多少资金？”

新的风险快速涌现，加之实施知识产权侵权的渠道日益增多，意味着风险缓解不能一蹴而就，需要持续的分析和监控。越来越多的企业正在寻求外包合作伙伴的帮助，以应对这一挑战。

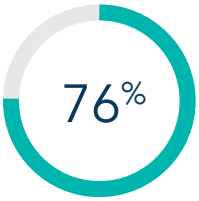
> 平台更迭之快令人应接不暇：年轻一代使用的平台正逐渐取代我们今日所依赖的平台，并将成为我们明日使用的工具。形势瞬息万变，但我们不能慢人一步。这必须引起重视，也意味着我们必须主动出击，而不是被动应对。
>
> **——Elliott Champion，CSC 品牌保护和反欺诈全球产品总监**

打击知识产权侵权需要全面、多团队协作的思维模式

受访者表示，他们对自身的监控和域名管理策略持较高信心。大多数（86%）受访者表示他们与其他团队（包括 IT 和安全团队）密切合作。



的受访者表示，**他们对企业内部的知识产权侵权监控系统“极其”或“相当”有信心。**



的受访者表示其企业已制定了域名管理策略，另有12%的受访者表示相关策略正在制定中。

然而，只有16%的受访者表示，他们的法务团队“完全”了解企业域名组合的管理情况。

“企业需要这种协调一致的方法来处理后端安全问题，尤其是在营销部门计划使用自有域名开展特定营销活动时。”Mary Jo 表示，“他们需要确保法务、安全和 IT 团队都了解该计划，以便将其添加到监控列表中。”

数字治理团队的兴起

在打击知识产权侵权方面采取主动措施并取得成功的企业，更有可能组建起正式的数字治理团队，成员为来自法务、营销、IT 和安全等部门的代表。

Elliott 表示：“在许多大型企业中，法务部门负责人很少与 IT 部门负责人沟通。他们彼此不了解对方的工作领域。我们对新客户说的第一件事就是，必须让所有相关人员聚在一起，以便从多维视角审视问题。

我最想强调的一点是，不同团队之间应该互相沟通，形式不必拘泥，甚至可以比月会更轻松随意，关键在于保持信息畅通。”

外包服务使用增多，包括域名监控

随着知识产权侵权数量持续攀升，企业内部人员越来越难以负荷域名监控及其他活动的工作量。这些工作通常由法务团队承担，而他们可能已经不堪重负。

超过半数（56%）的受访者表示目前已将部分监控业务外包，而且正积极考虑外包更多业务。

与信誉良好、经验丰富且专业的合作伙伴携手，不仅能减轻法务团队的压力，还能彰显企业致力于保护客户权益、恪守监管标准的承诺。同样重要的是，此类合作可以强化协议和防御措施，并提供创新工具和应用程序的使用渠道，从而带来显著价值。

“如果您面临商标侵权诉讼，而过去并未对商标滥用情况进行监控，那么法院不会作出对您有利的裁决。”Mary Jo 表示，“同理，如果今天再次面临类似诉讼，您可以指出自己正在与像 CSC 这样的合作伙伴合作，他们能够扫描交易平台、下架侵权内容，并尽可能增加不法分子的作案难度。简而言之，就是说明您正在竭尽全力保护知识产权。”

CSC 是领先的主动威胁防范工具提供商，这些工具能够识别可能成为网络攻击起跳板的潜在域名。通过快速、主动地在全球范围内采取行动，企业可以有效防范始于虚假域名的知识产权侵权。

“面对知识产权侵权威胁时，负责任的企业必须建立多层次、主动式的网络安全防御体系。仅安装防火墙远远不够。如果您尚未考虑将知识产权侵权监控和域名管理策略外包，则意味着您已错失优势。”

——Ian McConnel，CSC 首席法务官

零售级注册商与企业级注册商有何区别?

在评估如何监控和保护域名时，了解零售级注册商和企业级注册商之间的区别至关重要。Ihab 指出了五大关键区别：

1. **维权能力：**企业级注册商可提供覆盖全球、高效且智能的维权（或下架）服务，而零售级注册商缺乏相应的工具和专业能力。
2. **业务重心：**零售级注册商主要作为中间商销售域名，企业级注册商则专注于域名管理和保护以及全球风险管控。
3. **托管安全：**零售级注册商虽可提供用于托管域名的网络服务器，但这些服务器往往维护不足，并且可能依赖不安全的共享基础设施。
4. **安全防护：**企业级注册商会采取更强大的安全措施来保护客户的域名组合，其防护能力非零售级注册商可比。
5. **监控范围：**企业级注册商会监控全球电商及拍卖网站，及早发现域名滥用行为，而零售级注册商通常只有在问题暴露后，才会采取行动。

“欺诈者主要通过三种手段攻击品牌所有者：品牌滥用、身份仿冒和假冒产品。”Ihab 指出，“要有效应对这些威胁，必须与拥有强大维权团队的企业级注册商合作，任何低于此标准的方案都不足以解决问题。”

采取行动，刻不容缓

针对企业知识产权的攻击数量不同攀升，形式不断出新。由于 AI 和 CaaS 工具包等技术的出现，欺诈者的作案门槛大大降低。我们的研究表明，法律专业人士普遍认为，他们已建立了妥善的政策和协作机制来应对风险。然而，若缺乏多层次、主动式的网络安全防御体系，将会越来越难以应对不断升级的威胁。

与值得信赖的第三方合作，构建主动式安全防御体系，既能为知识产权保护开辟清晰有效的路径，又能向客户及利益相关者表明企业已部署适当的保障措施，让他们安心。

Mary Jo 表示：“主动防御彰显企业对资产与知识产权的重视。从长远来看，这种投入定能带来回报，不仅体现在侵权检测和监控方面，还在于它能确保您已部署合适的法律维权和下架机制。”

采取主动姿态，特别是与经验丰富的第三方合作，还能更有效地利用时间和资源。

Elliott 总结道：“不主动防御的后果是必须做更多补救工作。拿取回域名来说，与 CSC沟通五分钟或许就能解决，但在没有企业级提供商的帮助下，您可能需要耗费五个月的时间，再搭上额外费用。”

最后，Ihab 强调了知识产权保护与财务风险和声誉风险之间的关联。

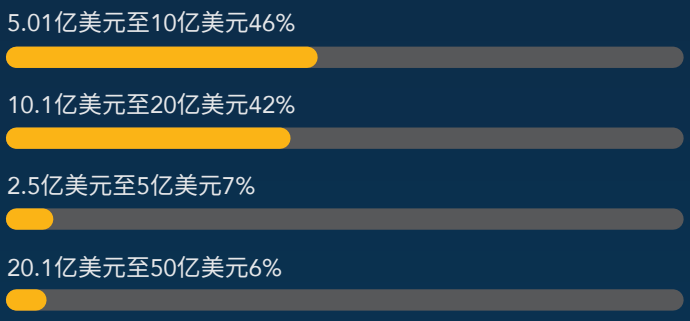
“知识产权与声誉密不可分，因为企业声誉如今取决于其在线形象。面对大量涌现的新型威胁载体，必须采取有别于以往的防护措施。”

受访者概览

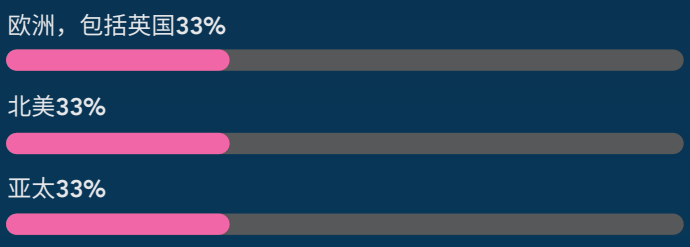
按垂直行业划分的公司数量

受访者职衔

公司年收入



按区域划分的公司总部



联系我们

+86 21 63913188 | cscdbs.com/cn

CSC 简介

CSC 是值得信赖的优选安全和威胁防范提供商，深受福布斯全球企业2000强和全球最佳品牌100强(Interbrand®) 企业的青睐，专注于域名安全和管理以及数字品牌和欺诈防护业务。随着全球越来越多的公司加大投资力度完善安全状况，我们的 DomainSec℠ 平台可以一展身手，帮助这些公司了解他们存在的网络安全漏洞并且保护其在线数字资产和品牌。企业可以凭借 CSC 的专有技术来增强自身的安全状况，防范针对其在线资产和品牌声誉的网络威胁，从而避免遭受严重的收入损失。CSC 还提供在线品牌保护（将在线品牌监控和维权活动相结合），多维度审视防火墙外针对特定域名的各类网络威胁。欺诈防护服务可在攻击的早期阶段打击网络钓鱼，使我们的解决方案更加完善。CSC 成立于1899年，总部位于美国特拉华州威尔明顿市，在美国、加拿大、欧洲和亚太地区设有办事处。CSC 是一家全球性公司，我们通过聘用所服务行业的业内专家，可为世界各地的客户提供服务。欢迎访问 cscdbs.com/cn。

DBS10222025