CSC

The IP Frontiers Report 2025

Proactive security against IP infringement

Introduction: A fast-changing, high-risk world

A company's reputation is very closely tied to how it's represented online. This creates opportunities for fraudsters to exploit well-known brands—whether by launching deceptive websites, copying products or logos, or setting up fake social media profiles that mimic the brand.

The barriers to entry for impersonators have been reduced significantly, making intellectual property (IP) infringement easier to carry out than ever before. IP infringement is becoming increasingly difficult to identify and pursue, and offenders are not always responsive to cease-and-desist letters alone.

To address these challenges, enterprises benefit from employing a range of tactics to strengthen IP enforcement and protect their trademarks, copyrights, and other intellectual property rights.

At a time when legal teams' resources are increasingly stretched, how should they work more closely with marketing, IT, and security teams to prioritize efforts in IP protection and ensure that budgets are directed in the right direction?

"The ability for fraudsters to carry out IP infringements is iterating at such a pace that it will be to everyone's benefit to be more aware of what's happening, to be more technology-focused, and to foster stronger collaboration among teams involved with domains," says Ian McConnel, CSC chief legal officer. "Like it or not, domain management is a key part of cybersecurity strategies, not just protecting the crown jewel domain names."

OUR EXPERTS

Ian McConnel
CSC Chief Legal Officer

Ihab Shraim
Chief Technology Officer,
CSC's Digital Brand Services division

Elliott Champion
CSC Global Product Director,
Brand Protection and Anti-Fraud

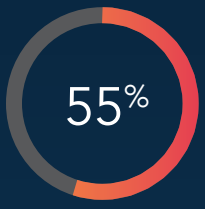
Mary Jo Murphy
CSC Product Manager,
Brand and Fraud Services

Key takeaways from our research

We surveyed 300 senior legal professionals in Q2 2025 and found that:

The rate of online IP infringement is increasing, and predicted to grow

The vast majority of respondents (91%) said they were concerned about the threat of online IP infringement.



More than half (55%) said they expect a significant increase in online IP infringement over the next three years.

Respondents listed the top three types of online IP infringement they've experienced as:

Counterfeiting

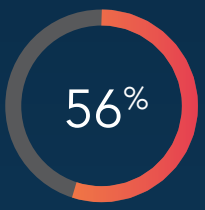
Trademark abuse

Impersonation

AI plays an important role in rising IP infringement

A majority (88%) said artificial intelligence (AI)-enabled systems are driving an increase in the frequency of infringements.

Respondents recognize the benefits of outsourcing online IP infringement monitoring



More than half (56%) said they currently outsource some online IP infringement monitoring activity but are actively looking at outsourcing more.

Most legal teams are already collaborating with IT and security teams to understand IP infringement risks in detail

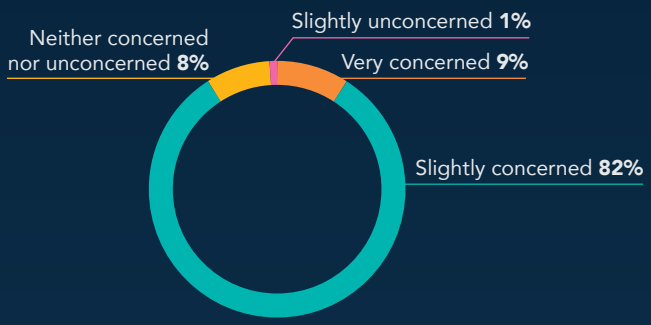
Nearly two-thirds (64%) rated their collaboration with IT security colleagues as strong (four points out of five), **while a further 22%** said they work extremely closely with their IT security team.

The occurrence of IP infringement continues to rise

A number of catalysts have come together over the past few years to profoundly impact the world of IP infringement.

This diverse range of drivers includes the rise of crimeware-as-a-service (CaaS) kits, the ongoing increase in cost of living, and continued growth in online shopping—all of which are fueling IP infringement and damaging company reputations and profits as a result.

Tellingly, more than 90% of respondents to CSC's global survey said they were concerned about the threat of online IP infringement on organizations such as theirs.



A quarter said they had seen a "significant" increase in online IP infringement faced by their organization over the past 12 months; around a third (35%) said they had seen a "significant" increase over the past three years.

Respondents reported the top three exploited assets as:

- Internet content or branded content (cited by 45%)
- Mobile apps (30%)
- Online marketplaces (17%)

"People are always looking for cheaper products, such as pharmaceuticals, automotive parts, and consumer goods—and fraudsters are taking full advantage," says Mary Jo Murphy, CSC product manager, Brand and Fraud services.

Looking ahead, most respondents (89%) said they expect an increase in IP infringement over the next three years. Nine in 10 (90%) also expect an increase over the next 12 months.

Which of the following types of online IP infringement are of most concern to your organization?

- Counterfeiting
- Trademark abuse
- Impersonation
- Design right abuse
- Copyright abuse

"The way you view these types of infringements depends on your perspective," adds Ian. "If I'm a consumer-based company, I'd be the most worried about counterfeit goods, but if I'm a financial services company, I'd be more worried about a fraudster misappropriating a trademark to facilitate a phishing or cyber attack on a client."

> Your reputation is represented by your online presence, which means you have to guard your reputation differently than in the past. There's a massive influx of threat vectors targeting corporations, and the easiest targets for them to attack are domain names and IP. What's changed is that in the past, fraudsters would send hundreds of thousands of phishing emails hoping that 2% or 3% would respond, while today fraudulent activity is more targeted and comes with a much higher rate of success.
>
> **– Ihab Shraim, chief technology officer, CSC's Digital Brand Services division**

THE IMPORTANCE OF PROTECTING DOMAIN NAMES IN THE FIGHT AGAINST IP THEFT

"Domain names are a core element of how everyone interacts and communicates with each other day to day. It's so common that people don't even realize they're interacting with a domain name and take it for granted that they're staying safe from harm. Yet fake web domain names are often the starting point for serious IP infringement, and it has never been easier for fraudsters to register any domain name they choose," says Elliott Champion, CSC global product director, Brand Protection and Anti-Fraud.

"Have you noticed how at some restaurants you now use a QR code to order? When you scan it, it takes you directly to a domain name and you have no idea where it's going—you just trust it," Elliot explains. "That's how critical domain names are to the daily digital experience. We all trust and interact with them, even though it can take just a few minutes to set up a fake name. It means the barriers to entry for this type of fraudulent activity are now unbelievably low."

AI is playing an increasingly powerful role in IP infringement

In record time, AI has come to dominate much of the global business and productivity narrative. But on the flip side, from a fraud and risk perspective, AI is already being used to create highly realistic and sophisticated IP assets such as logos, pictures, and corporate content. As AI and AI-led capabilities continue to accelerate, the deep concern for legal teams is how best to detect risks and stay ahead of the curve.

Unsurprisingly, around nine in 10 respondents (88%) to our survey said AI-enabled systems are driving an increase in the frequency of incidents.

The majority of respondents (93%) also said they were concerned that the ability to use AI to create fake assets could materially impact their business.

"It takes no effort at all today to go to an AI-powered tool and have it create fictitious materials that can be leveraged very easily," says Ian. "The days of having to sit down and code a bunch of fake web pages are over, and as tools get even more sophisticated, the opportunities for less tech-savvy bad actors will continue to grow. Fraudsters are only limited by their imagination."

Firms are experiencing the new and evolving AI-driven challenges. Nine in 10 respondents also said they are concerned that AI tools might use their organizations' data or IP to train models that could generate content usable by competitors—however, the majority of respondents who have this concern believe they have adequate protections in place.

One positive sign is that many firms recognize the escalating AI threat and are bolstering defenses with internal training programs and other initiatives.

Almost 70% of respondents report they rate the quality of the internal guidelines or policies their organization has in place for the use of AI in the creation of IP assets as good, while 20% rate theirs as excellent.

Looking ahead, training will likely form an increasingly important role in how enterprises prevent AI-led risks.

DISTINGUISHING FACT FROM FICTION IS BECOMING MORE CHALLENGING

One of the top three concerns for respondents regarding IP infringement is impersonation, including realistic AI-generated portrayals of senior executives that can be used to request funds from employees.

"There's enough content out there of CEOs, including speeches, posts, and videos that fraudsters can use to create AI representations within hours, that would fool many people in an organization," says Ian. "At some point, we'll be looking at an online representation of somebody that will look exactly like the person we interact with regularly, and we'll have no ability to differentiate truth from fiction.

"It's not here today, because you can still see fake video chats are a little off, but it's iterating so fast and improving at such an exponential rate that, honestly, it's just a matter of time.

"It will mean organizations will need to have processes and systems in place that don't solely rely on the individual to authenticate communication, whether that's by phone, video, or email. In five years' time, there will be no training that will work to stop these fraudsters.

"Fighting back starts with taking down domain names that may launch these sorts of communications and having the right protocols in place to verify where illicit communications are coming from."

Budgets are growing, but spending is not always prioritized

In a world where the number and type of risks and catalysts continue to escalate, how have dedicated IT budgets shifted to meet the challenge?

Our study found that budgets for IP infringement and brand protection are increasing—two thirds (67%) of respondents said they expect them to increase "significantly" over the next three years while just under half (46%) predict a "significant" increase in the year ahead.

Over the next 12 months, respondents expect the areas that will see additional investment are:

72%	69%	68%
In-house technology	Higher IP management team headcount	Headcount growth of the wider legal department

Almost half (44%) expect greater outsourcing to dedicated IP specialist third parties, similar to CSC.

These rising investments highlight an important question—where should resources be directed to have the greatest impact? Rather than attempting to cover every potential channel or variant of a domain name, enterprises should prioritize spending on where it will make the most difference.

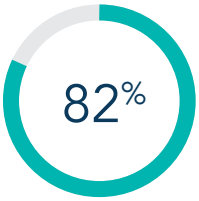
"It's not just a matter of increasing budgets, but also how those budgets are spent," says Ian. "How much are you spending to become up to speed on issues relating to AI? How much are you spending on getting the right resources in place to properly mitigate the risks?"

The rapid emergence of new risks, combined with the growing number of channels used to launch IP infringement, means that mitigation cannot be a one-time effort but requires continual analysis and monitoring. Increasingly, organizations are turning to outsourced partners to help meet this challenge.

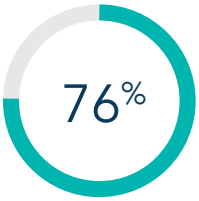
> The platforms shift so fast—what we rely on today is already being replaced by what younger audiences are using, and that's what we'll be using tomorrow. The map is always moving, and you're always slightly behind the curve. So, it's something that needs attention and means you have to be proactive rather than reactive.
>
> **– Elliott Champion, CSC global product director, Brand Protection and Anti-Fraud**

Combating IP infringements needs a comprehensive, multi-team mindset

Our respondents reported having relatively high confidence levels in their monitoring and domain management strategies, and most (86%) say they work closely with other teams including IT and security.



of respondents said they were either "extremely" or "fairly" confident with their organization's in-house IP infringement monitoring systems.



said their organization has a domain management strategy in place, with a further 12% in the process of creating one.

However, only 16% reported that their legal teams have "total" visibility into the management of their organization's domain portfolio.

"Organizations need this cohesive approach to deal with back-end security issues, especially when marketing is planning to launch a specific campaign with its own domain name," says Mary Jo. "They need to make sure legal, security, and IT teams are aware it's coming so they can add it to the monitoring list."

THE EMERGENCE OF DIGITAL GOVERNANCE TEAMS

Organizations with a successful, proactive approach to battling IP infringement are more likely to have assembled an official digital governance team, made up of representatives from legal, marketing, IT, and security.

"In many large organizations, the head of the legal department doesn't often speak to the head of the IT department," says Elliott. "They don't understand each other's worlds. The first thing we say to new clients is that we need to get you all in a room so you can see this problem from different perspectives.

"If there's one message I'd want to get out there it's for the various teams to speak to each other—it doesn't even have to be more formal than a monthly meeting, but it's vital to keep each other informed."

Greater use of outsourcing services, including domain name monitoring

As the number of IP infringements continues to rise, the effort required to monitor domain names and other activities becomes more difficult to manage in house. Such activities are often the responsibility of the legal team, which may already be at capacity.

Just over half (56%) of respondents said they currently outsource at least some monitoring activity but are actively looking at outsourcing more.

Partnering with a reputable, established, and dedicated specialist not only alleviates pressure on legal teams but also demonstrates a commitment to protecting customers and meeting regulatory standards. Equally important, such partnerships can deliver significant value by strengthening protocols and defenses, while providing access to new, innovative tools and applications.

"If you find yourself fighting a trademark infringement case, the courts would not look favorably on you if you were not monitoring the misuse of your trademarks in the past," says Mary Jo. "In a similar way today, you can point to the fact you're working with a partner like CSC that can scan the marketplaces, take down infringements, and make it as difficult as possible for bad actors—quite simply as a way to show you're doing everything you can to protect your IP."

> CSC is a leader in providing tools that enable proactive threat intelligence on potential domain names that may be the launching point for an attack. Being able to do that quickly, proactively around the world, helps companies guard against IP infringement that starts with fake domain names.
>
> "A responsible company facing IP infringement threats needs to have a multi-layered, proactive cybersecurity posture. Just having a firewall in place is not enough. And if you haven't looked at outsourcing IP infringement monitoring and domain management strategies, then you're missing out."
>
> **– Ian McConnel, CSC chief legal officer**

RETAIL REGISTRARS VERSUS CORPORATE REGISTRARS—WHAT'S THE DIFFERENCE?

Understanding the differences between retail and corporate registrars is essential when evaluating how to monitor and protect domain names. Ihab highlights five key distinctions.

1. **Enforcement capability:** Corporate registrars provide global, effective, and intelligent enforcement (or takedowns), but retail registrars lack the tools and expertise to deliver.
2. **Business focus:** Retail registrars primarily exist to sell domain names, acting as intermediaries, while corporate registrars are dedicated to managing and protecting a domain name and mitigating global risks.
3. **Hosting security:** Retail registrars may offer web servers to host domains, but these are often inadequately maintained and may rely on insecure, shared infrastructure.
4. **Security posture:** Corporate registrars have more robust security measures to protect clients' domain portfolios—safeguards that retail registrars cannot match.
5. **Monitoring reach:** Corporate registrars monitor eCommerce and auction sites worldwide to detect misuse of domain names, while retail registrars usually act only after a problem has been identified.

"Fraudsters target brand owners with three main tactics: brand abuse, impersonation, and counterfeit products," notes Ihab. "To address these threats effectively, you need a corporate registrar with an enforcement arm—anything less falls short."

A time to act, before it's too late

The volume and variety of attacks on organizations' IP continue to rise. The barriers to entry for fraudsters are much lower due to technology like AI and CaaS toolkits. Our study shows that legal professionals are generally confident they have the right policies and collaborative working practices in place to address those risks. However, without a multi-layered, proactive cybersecurity posture, it will become more and more difficult to keep up with escalating threats.

Working with a trusted third party to help set up a proactive security posture creates a clear, effective path to IP protection, while assuring customers and stakeholders that proper safeguards are in place.

"Being proactive shows you value your property and your IP," Mary Jo states. "In the long run, it pays off—not only through detection and monitoring, but also by ensuring you have the right legal enforcement and takedown mechanisms in place."

A proactive approach, particularly in partnership with an experienced third party, is also more efficient with time and resources.

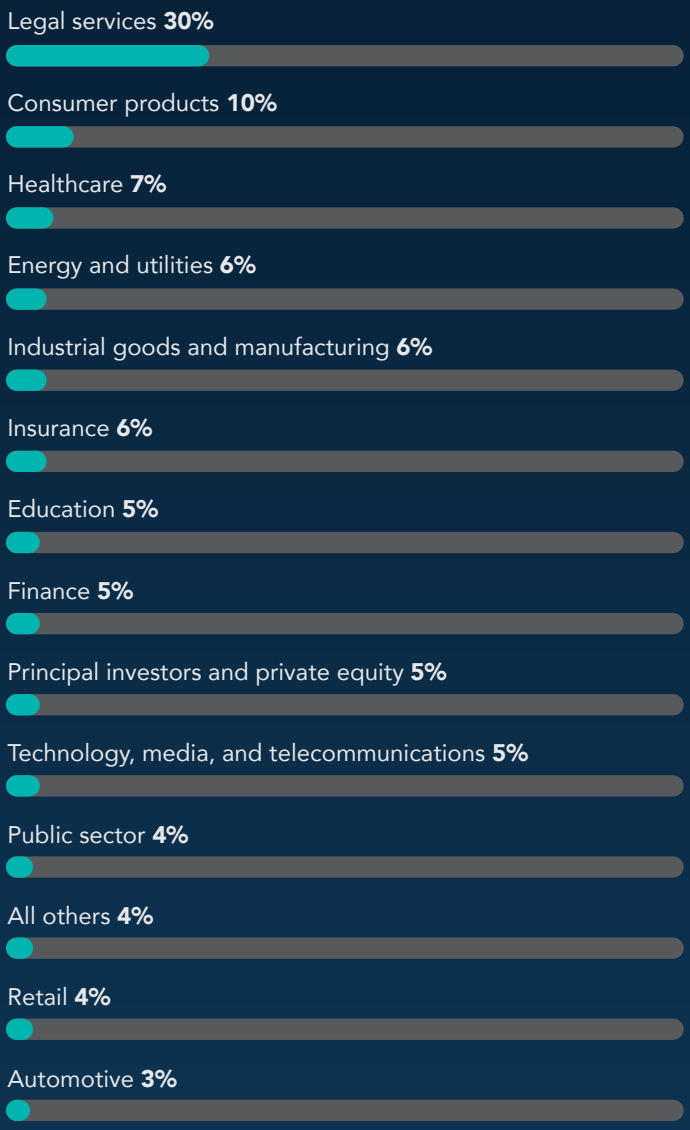
"The consequence of not being proactive is that you have to do more remediation," concludes Elliott. "What could take five minutes in a discussion with CSC might take you five months and additional expense to get a domain retrieved without the help of an enterprise-class provider."

Finally, Ihab underscores the connection between IP protection and financial and reputation risk.

"IP is inseparable from reputation, because your reputation now depends on your online presence. It must be protected differently today than in the past, given the massive influx of new threat vectors."

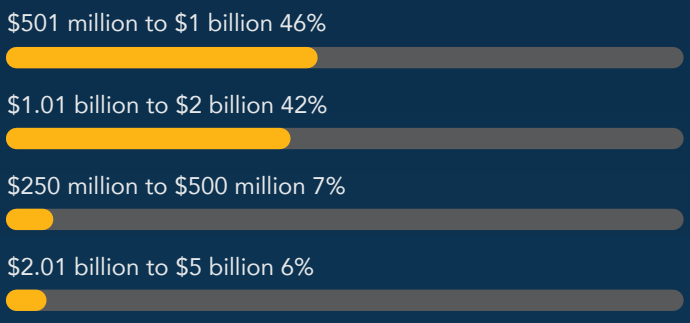
Overview of our respondents

Number of companies by vertical sector

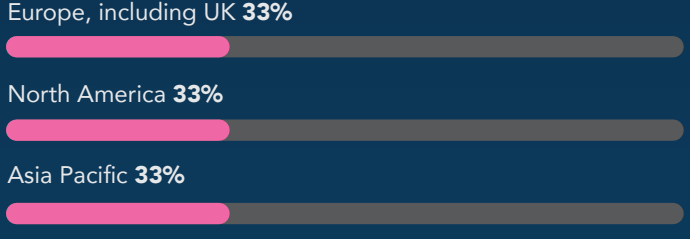


Job title of respondents

Annual revenue of companies



Headquarters of companies by region



Let's talk 1 800 927 9800 | cscdbs.com

About CSC

CSC is the trusted security and threat intelligence provider of choice for the Forbes Global 2000 and the 100 Best Global Brands (Interbrand®) with focus areas in domain security and management, along with digital brand and fraud protection. As global companies make significant investments in their security posture, our DomainSec℠ platform can help them understand cybersecurity oversights that exist and help them secure their online digital assets and brands. By leveraging CSC's proprietary technology, companies can solidify their security posture to protect against cyber threat vectors targeting their online assets and brand reputation, helping them avoid devastating revenue loss. CSC also provides online brand protection—the combination of online brand monitoring and enforcement activities—with a multidimensional view of various threats outside the firewall targeting specific domains. Fraud protection services that combat phishing in the early stages of attack round out our solutions. Headquartered in Wilmington, Delaware, USA, since 1899, CSC has offices throughout the United States, Canada, Europe, and the Asia- Pacific region. CSC is a global company capable of doing business wherever our clients are—and we accomplish that by employing experts in every business we serve. Visit cscdbs.com.

DBS10222025