



Anti-counterfeiting and Online Brand Enforcement: Global Guide

2023

**Securing your online brand: A
step-by-step guide to conducting a
comprehensive brand risk assessment**

Anti-counterfeiting and Online Brand Enforcement: Global Guide


2023

Now in its 16th year, *The Anticounterfeiting and Online Brand Enforcement: Global Guide* combines the latest strategic analysis with practical, country-by-country exploration of the best protection around the world, enabling brand owners to stay one step ahead of the counterfeiters.

Generated: May 13, 2024

The information contained in this report is indicative only. Law Business Research is not responsible for any actions (or lack thereof) taken as a result of relying on or in any way using information contained in this report and in no event shall be liable for any damages resulting from reliance on or use of this information. Copyright 2006 - 2024 Law Business Research



Explore on [WTR](#) 

Securing your online brand: A step-by-step guide to conducting a comprehensive brand risk assessment

Tim Brown

Com Laude

Summary

INTRODUCTION

SUMMARY AND CONCLUSIONS

INTRODUCTION

In today's ever-evolving digital landscape, brands encounter myriad risks online, encompassing trademark infringement, counterfeiting, online scams, malware distribution and phishing attacks. While attention often shifts towards headline-grabbing technologies like the metaverse, web3, blockchain and NFTs, it is essential to remember the enduring significance of domain names as a primary gateway for brand visibility and customer interaction.

Effective domain portfolio management is a frequently underestimated element of brand protection, despite its pivotal role in supporting a brand's online presence. With the ever-changing nature of the domain name space, brands often face challenges in keeping up with these developments and adjusting their online strategies accordingly.

One of the key concepts is understanding the distinction between first-party and third-party domains.

First-party domains refer to the domains directly owned and controlled by the brand itself, representing its official online presence. These domains are crucial for building brand reputation, fostering customer trust and delivering a consistent brand experience.

On the other hand, third-party domains are owned by external entities but may contain brand-related content, including unauthorised use of trademarks, counterfeit goods, misleading information or even malware and other criminal content.

DOMAIN NAMES – A BRIEF INTRODUCTION

The domain name system (DNS) was introduced in 1985. The DNS revolutionised the way users interact with the Internet by replacing cumbersome IP addresses – like 94.199.146.95 – which servers use to communicate, with user-friendly domain names that are easier to remember and type into a browser. The DNS was designed to make internet services easily discoverable and accessible.

In the early days of the commercial Internet, the domain name space was relatively limited, with just a handful of top-level domains (TLDs) such as '.com', '.org' and '.net'. However, as the Internet quickly gained traction and businesses and individuals rushed to establish their online presence, the demand for domain names skyrocketed.

Recognising the need to expand the domain name space to accommodate the growing naming system, the Internet Corporation for Assigned Names and Numbers (ICANN) was established in 1998 in California. ICANN, alongside the Internet Assigned Numbers Authority (IANA), were made responsible (among many other things) for root zone management in the DNS.

In plain English, this means that ICANN is responsible for the TLDs that appear at the right-hand side of the domain names in your browser's address bar.

Over the years, ICANN has overseen several rounds of TLD expansions, introducing new generic top-level domains (gTLDs) to cater for specific industries, interests and geographic locations. The first new TLDs were added to the root in around 2001. These included spaces like '.biz', '.info' and '.museum'.

The process of adding new spaces was not entirely straightforward and so ICANN looked in detail so new domains could be added to the root quickly and easily. The result was the new gTLD programme which came about in 2012 and which saw about 1,400 new TLDs being added to the root. These are known as 'new' gTLDs (even though many are now over ten years old).

While ICANN is responsible for a huge part of the domain name space; its responsibility only covers gTLDs. Brand owners must also consider country-code top-level domains (ccTLDs). These are domain name spaces that represent individual countries or territories. They typically consist of two letters that correspond to the country's International Standards Organisation's (ISO) two-character country codes (encompassed by ISO3166-1).

As is always the case in the domain name space, there are exceptions. For example, the ISO's country code for Great Britain is 'GB'. But, back in the 1980s the Joint Academic Network (also known as JANET, which now operates '.gov.uk') had its own domain name system called the Name Registration Scheme, which used '.uk' in its naming format. Early Internet adopters were therefore used to '.uk' and so it remained, rather than the ISO's '.gb' being adopted.

In addition to denoting geographic origin, ccTLDs often have specific policies and regulations set by the respective country's domain name operator. These policies can include restrictions on who can register a domain name under a ccTLD, requirements for local presence or documentation, and rules regarding trademark protection. Keeping on top of these shifting rules and regulations quickly becomes extremely complicated.

Today, the domain name space is a dynamic ecosystem encompassing hundreds of gTLDs, ccTLDs, sponsored, community and brand TLDs. And it continues to evolve and develop as new technologies and trends emerge, including blockchain-based domains, decentralised web platforms and alternative non-ICANN controlled DNS systems.

EFFECTIVE FIRST-PARTY DOMAIN NAME MANAGEMENT

Given this background of hundreds of top-level domain name spaces and a shifting regulatory environment, brands often have difficulties maintaining an effective domain name portfolio that is fit for purpose. A poorly managed, misdirected portfolio is entirely at odds with best practice for effective brand protection and security. Equally, maintaining a large and unnecessary portfolio wastes resources, both in terms of time and money.

As businesses evolve and expand, it is essential to ensure that the domain portfolio aligns with these evolving needs. Just as business strategies adapt to changing market dynamics, an effective domain portfolio should reflect the growth and transformation of the brands it protects.

A BLOCKING PORTFOLIO?

Registering and blocking every conceivable domain variant as a defensive measure is not only outdated but also costly.

Firstly, as outlined above, the domain name space has expanded significantly over the years. This means that the number of potential domain variations has multiplied, making it virtually impossible to register and block every conceivable variant. The sheer volume of domain names that would need to be registered and maintained simply makes this old-fashioned approach impractical and financially prohibitive.

Secondly, any such defensive strategy does not effectively address the evolving tactics of malicious actors. Cybercriminals are adept at quickly adapting and creating new variations to bypass these traditional defensive measures. In effect, attempting to block every possible domain variant becomes a never-ending and futile task, as new variants and combinations emerge.

WEED OUT OBSOLETE DOMAIN NAMES

One common challenge faced by all brands is the accumulation of 'dead wood' in their domain portfolios. These are obsolete domains that are no longer actively used or necessary for supporting brands. Think domain names reflecting advertising straplines that have long been discontinued; brands that no longer exist or domain names registered in irrelevant spaces.

These unused domains clutter the portfolio, creating potential confusion and presenting security risks. Moreover, domains that do not resolve or lead to irrelevant content can confuse or frustrate users and potentially be exploited for malicious purposes.

In terms of the latter, it is relatively easy to spoof a domain name so that it appears that email has been sent from that domain. Spoof email addresses can be used for all sorts of criminality. These attacks are far more effective if carried out through the targeted brand's own, unused, domain names.

COMMON TYPES OF DOMAIN CRIMINALITY

- **Phishing:** Cybercriminals use spoof email addresses to send fraudulent emails that appear to be from legitimate sources, such as banks, e-commerce platforms or government agencies. These emails often trick recipients into providing sensitive information like passwords or credit card details that can then be further exploited for financial fraud or identity theft.
- **Business email compromise (BEC):** Spoof email addresses are commonly employed in BEC scams, where attackers impersonate executives, partners or suppliers to trick employees into performing fraudulent financial transactions. These often involve wire transfers, invoice manipulation or redirecting funds to attacker-controlled accounts.
- **Malware distribution:** Spoof domains are used to distribute malicious attachments or links that, when opened or clicked, instal malware on the recipient's device. This grants unauthorised access to sensitive data, allows remote control of the device or is used to launch further cyberattacks.
- **Advance fee fraud:** Also known as 419 scams (419 refers to the section of the Nigerian Criminal Code that deals with fraud; these types of fraud having originated in Nigeria), these attacks involve convincing victims to send money or provide personal information in exchange for a promised reward or financial benefit. Again, spoof email addresses are commonly used to initiate communication and build trust with the victims.
- **Harassment or impersonation:** Spoof domain names can be used to harass individuals, tarnish reputations or impersonate executives and other staff members for malicious purposes. This can include sending threatening or abusive messages, spreading false information or carrying out targeted harassment campaigns.

'Dead wood' or obsolete domain names should be considered for lapsing or at least the domain name manager should ensure that appropriate email authentication protocols are implemented. These measures included the application of protocols like Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-Based Message Authentication, Reporting and Conformance (DMARC). These protocols help verify the authenticity of incoming emails by checking the sender's domain against the authorised email servers.

CONSOLIDATION OF SUPPLIERS

Managing a domain portfolio becomes even more complex when different providers are involved for registrar services (RSP), SSL certificates and nameservers (NS).

Successful brands enlist the help of a reputable company specialising in domain portfolio management. Such companies have the expertise and tools to streamline portfolio management, ensure security compliance and provide valuable guidance based on industry best practices. Such companies work for brand holders' interests (rather than against them) to assist in rightsizing and regularly clearing the portfolio, identifying redundant domains and optimising the brand's online presence.

By utilising the expertise of a reputable domain management company, brands can optimise their portfolio, allocate resources more efficiently, make sure the domain portfolio shows a demonstrable return on investment and ensure brands are defended online while deploying modern security and marketing best practices.

THE JIGSAW APPROACH TO BRAND PROTECTION

As we have discussed, there are myriad ways in which criminals exploit online spaces to attack brands. To effectively manage these risks, brands must employ a variety of methods for identifying potential threats. Chief among these is the need for a proactive brand monitoring service.

Brand protection requires a comprehensive and multifaceted approach to effectively safeguard intellectual property. Relying on a single provider for all aspects of brand protection may not yield the desired results. Instead, employing a jigsaw of service providers who excel in their respective areas, such as social media monitoring or domain name monitoring, is most effective.

Experience has shown that different facets of brand protection necessitate specialised knowledge, tools and techniques to identify and address specific risks. For example, social media monitoring involves tracking brand mentions, detecting counterfeit accounts and mitigating reputational risks arising from user-generated content. On the other hand, domain name monitoring focuses on identifying and prioritising domain-related infringements, cybersquatting and the myriad domain-related threats outlined above.

By utilising best-in-class service providers for each area, brands can harness the expertise and tailored solutions required to tackle the unique challenges posed by different platforms and mediums. Social media monitoring specialists possess the necessary tools and algorithms to navigate the vast landscape of social networks effectively. Similarly, marketplace monitoring requires specialist knowledge. It follows that domain name monitoring experts have in-depth knowledge of domain name registrations, trademarks, and legal and administrative processes.

Collaborating with multiple providers also offers the advantage of diverse perspectives and insights. Different providers bring their unique skill sets, technologies and methodologies, ensuring a holistic and robust brand protection strategy. This allows for comprehensive coverage, increased accuracy and more targeted responses to infringements or risks, which results in a better return on investment.

Ultimately, this jigsaw approach to brand protection acknowledges that no single provider can excel in every aspect of brand protection.

AUTOMATION ANSWERS THE PROBLEM...

Traditionally, domain name monitoring consisted of detecting and reporting newly registered domain names that potentially infringe the monitored brand.

However, simply gathering and presenting basic data is insufficient in today's fast-paced digital landscape. Brands must go beyond data collection and focus on assessing and evaluating the identified risks. This is critical to avoid an unfocused scattergun approach to reporting and, ultimately, enforcement.

Given the growing number of domain names in the domain name space and the variations of possible attack, it is almost impossible to manually keep on top of more than a few dozen potentially infringing domain names. Equally, as soon as a manual report is produced, it is out of date. Domain names will have dropped. New domain names configured. Configurations changed, so that previously inactive domain names have gone live and, indeed, vice versa.

So, to bring about a cost-effective return on investment, data collection, presentation and prioritisation must be automated through the effective deployment of brand-specific algorithms and artificial intelligence. These technologies enable brands to analyse vast amounts of data, identify patterns and detect potential risks more efficiently. Automated systems can process data in real-time, enabling timely responses and reducing the risk of overlooking critical threats.

...AT LEAST IN PART

While automation can significantly enhance risk assessment, the final enforcement decision should involve human judgement. Automated enforcement solutions may do the heavy lifting of identifying potential risks, but every enforcement decision requires human intervention.

It is crucial for brands to strike a balance between automated risk assessment and human decision-making, as overreliance on automated enforcement solutions can lead to unintended consequences.

For instance, when dealing with loyal fans or genuine resellers who may unintentionally infringe intellectual property rights, a human touch is necessary to make fair and proportional decisions.

Algorithms may not always understand the nuances of each situation and may inadvertently target legitimate entities or escalate minor issues. It is very important after all to avoid the 'Streisand effect'.

The Streisand effect refers to the unintended consequence of attempting to suppress or censor information that results in unintended attention and public interest in the very information that was meant to be hidden or suppressed. The phenomenon is named after a

2003 incident involving the American singer Barbra Streisand, where her attempt to suppress photographs of her house ended up drawing far more attention than if she had taken no action!

Therefore, human judgement is essential to ensure that enforcement actions are appropriate and aligned with the brand's overall objectives.

PRIORITISE, PRIORITISE, PRIORITISE

Prioritisation is a hugely important element of effective brand protection. Not all risks carry the same level of threat, and brands need to prioritise their enforcement efforts accordingly. Adopting targeted and smart enforcement strategies yield better results than relying solely on the scattergun approach of aggressive and very broad enforcement measures.

By focusing resources on high-priority risks – using a combination of automation and human insight – brands can maximise their impact and demonstrate the most effective return on investment.

COMBINE FIRST-PARTY AND THIRD-PARTY STRATEGIES

Having discussed first-party and third-party domain names, it is important to ensure that brands have a joined up strategy for both. This is an often-overlooked element of effective online brand protection. Frequently, responsibility for the technical aspects of managing a domain name portfolio and intellectual property enforcement lie with different functions. But one cannot exist in isolation from the other.

Therefore, developing and implementing joined-up risk mitigation strategies across both first-party and third-party domain names is critical. Working with a reputable CDM provider can greatly assist in policy development and implementation.

To begin with, it is essential to identify any gaps in the domain portfolio. This means evaluating the brand's online presence and assessing whether all relevant domains are registered and actively managed. Gaps may arise due to missed registrations – either in gTLDs or ccTLDs – expiration of domains or the emergence of new brands. By regularly conducting thorough analyses, brands can identify potential vulnerabilities and take proactive measures to fill these gaps.

In addition to addressing gaps, it is important to ensure that the domain portfolio is functioning properly. This involves regular monitoring and evaluation of all domains to ensure they are actively serving their intended purpose. Domains that are not effectively utilised or no longer relevant may create opportunities for criminals to exploit them for the fraudulent activities noted above. By regularly assessing the performance of each domain and addressing any issues promptly, brands can minimise the risk of exploitation.

Equally, registration policies should be planned and implemented, encompassing domain registration, management and renewal guidelines. These should be considered alongside the strategy and procedure for handling potential infringements and unauthorised use of the brand's intellectual property. In other words, any policies must align registration and enforcement activities.

MAKE THE MOST OF THE PORTFOLIO

As well as making sure that every domain name in a portfolio is pulling its weight by directing customers to legitimate active content, it is important to ensure that domain names recovered through enforcement or acquisitions are put to use.

Recovered domain names can be valuable assets in brand protection efforts. Instead of leaving these domains dormant, brands can redirect them to educational resources or designated landing pages that provide information about the brand, its genuine products or services, and guidelines for consumers.

Criminals will often promote scams through social media or direct messages (say, in smishing attacks) that lead to infringing domain names. Once these domain names have been recovered, criminals will rarely – if ever – clean up any references to domain names on these channels. This can lead to a valuable long tail of references on social media, etc, to recovered domain names. Best practice is to use this traffic to educate and inform. This proactive approach not only helps educate users but also prevents potential confusion or any further misrepresentation.

MONITORING TO SHOW A RETURN ON INVESTMENT

Monitoring and reviewing brand protection efforts are crucial to stay ahead of evolving threats and ensure the best return on investment (ROI) for enforcement activities. The dynamic nature of the digital landscape necessitates continuous assessment and adaptation to effectively protect brand assets.

To demonstrate the value of brand protection efforts, it is essential to measure the ROI. Tracking metrics such as traffic through recovered domains, reduction in counterfeit sales or customer feedback can provide insights into the effectiveness of the brand protection strategy. By quantifying the impact of their actions, brands can justify the resources allocated to brand protection and make informed decisions on future enforcement strategies.

The online space is constantly shifting, with new technologies, platforms and trends emerging regularly. It is essential to monitor these developments and evaluate their potential impact on brand protection strategies. By staying informed about the latest threats and trends, brands can proactively adjust their systems and methodologies to effectively address emerging risks. This may involve reviewing and updating monitoring tools, enhancing security measures and adjusting enforcement strategies to align with evolving online behaviours.

In addition to monitoring external changes, it is equally important to regularly assess the effectiveness of brand protection efforts. This involves evaluating the ROI on enforcement activities to ensure that resources are allocated optimally and generate positive outcomes. By measuring the impact of enforcement actions, brands can determine the effectiveness of their strategies and make informed decisions about resource allocation.

To assess ROI, brands should track a variety of metrics, such as the number of infringements detected and resolved, measuring DNS traffic to recovered domain names, alongside assessing the overall impact on brand reputation.

This data provides valuable insights into the effectiveness of enforcement efforts and helps identify areas for improvement or reallocation of resources. Regular review and analysis of these metrics allow brands to optimise their brand protection strategies and allocate resources more efficiently.

The domain name space is dynamic and ever-changing, and monitoring and reviewing brand protection efforts must be an ongoing process, rather than a one-off exercise. By establishing a regular review cadence, brands can ensure that their systems and methodologies remain up to date and responsive to the latest challenges. This may involve periodic audits, engaging in proactive threat intelligence gathering and seeking feedback from stakeholders within and outside the organisation.

Collaboration with internal and external stakeholders is crucial for effective monitoring and review. Internal teams, such as legal, marketing and IT, should collaborate closely to share insights, identify potential gaps and align strategies. Externally, partnerships with brand protection service providers, industry associations and law enforcement agencies can provide valuable resources and expertise for monitoring and reviewing brand protection efforts.

SUMMARY AND CONCLUSIONS

In conclusion, effective brand protection is a multifaceted endeavour that requires specialised expertise and an approach tailored to each brand's requirements. One size doesn't fit all when it comes to protecting brands online, and relying on generalist solutions may leave critical gaps in security.

Being smart with enforcement budgets is crucial. Resources must be allocated efficiently to maximise the impact of enforcement activities. Technology plays a pivotal role in this process, as it enables automated monitoring, detection and analysis of potential infringements. By leveraging technology to handle the heavy lifting, brands can save time and resources while maintaining constant vigilance over an ever shifting online space.

However, it is essential to recognise that technology alone cannot make the final decisions in brand protection. While algorithms and artificial intelligence can assist in assessing risks and identifying potential infringements, the ultimate enforcement decisions should be made by experienced professionals.

This human touch ensures that enforcement strategies align with the brand's values, objectives and legal considerations. The robots have not taken over just yet.



Tim Brown

tim.brown@comlaude.com

<https://comlaude.com/>

[Read more from this firm on WTR](#)