Maximizing Domain Name Competencies Within Large Corporations

CSC_Corporate_**Domains**^{SM}

GLOBAL DOMAIN NAME MANAGEMENT

Introduction

Managing a multinational corporation's domain name portfolio can be extremely difficult given the fragmented nature of the domain name industry and the diversity of corporations' brands and global corporate structures. Specifically:

- **gTLDs:** Generic top-level domains (gTLDs) such as .com, .net .org, .info and .biz alone involve relationships with 4 registries. Registry operators maintain the list of available domain names within their extension and allocate those names on a first-come, first-served basis.

- **ccTLDs:** There are approximately 244 country code top-level domains (ccTLDs) with their own registry operator. These include government agencies, not-for-profit organizations and commercial entities. Each of these registries has different registration and management rules.

- **Registrars:** In addition, there are hundreds of ICANN-accredited registrars, some of which remain inactive. Registrars, such as CSC Corporate Domains, maintain contact with the client to register and manage their domain names, and act as the technical interface to the registry on the client's behalf. Often companies may have dispersed their domain name registrations across several registrars.

- **Registrants:** Internally, different individuals in different offices around the world and indeed, sometimes within the same office, may have historically registered domain names on behalf of the company. In these cases, the registration contact details may be inconsistent and as a result renewal applications, payment details and a variety of administrative tasks may be dispersed across different individuals and business units, resulting in mistakes, such as a domain name being deleted unintentionally.

- **Internal Strategies and Policies:** Once consolidated and standardized, corporations often need different individuals to manage brands and domain name registrations in different regions, action renewals and respond effectively to new TLD opportunities.

The competence to tackle the above and related issues is dependent on two key areas:

1) POLICY AND RESOURCE (ORGANIZATIONAL CAPABILITY)

- Policy: Defined procedures to govern how the domain name strategy will be executed.
- Resource (org capability): The resources to manage the portfolio and implement a strategy.

2) DOMAIN NAME STRATEGY

- A defined approach to meeting business, marketing and IT objectives in relation to online brand management.

Part 1 - Developing Policy and Resource Capabilities

A COORDINATING OR CENTRALIZED RESPONSIBILITY FOR DOMAIN NAMES

The planning and implementation of a successful strategy requires input and management from a number of different business divisions. These may include:

Legal

Often the overall responsibility of domain names lies with the trademark lawyers, as domain name portfolios are perceived as an online extension or variation of the trademark portfolio.

Marketing

Where domain names represent brands and marketing activities, brand managers and marketers will have a crucial role in determining which brands should be registered where. They will also have been key participators in any rebranding exercises.

Technical

IT and technical departments may also be involved, particularly when there are decisions relating to the DNS management of domains.

Global and Regional Offices

Where a company has offices in different territories, regional offices may be responsible for the domain names in their territory. To ensure the centralized management of the portfolio, the head office will commonly have the overall global responsibility.

Parallel with this is the necessity for clear policies to be made as to who can request and approve the various orders relating to domain names. These include:

- Registrations
- Renewals
- Modifications
- DNS changes

It may be that a number of individuals in various offices can request domain name registrations, but only key personnel in the legal department can actually approve the order. Similarly, different departments may have rights that are limited to different areas. For example, perhaps only the IT department will be able to request and approve DNS changes.

At this stage, a clear budget should be set for the implementation of further policies to manage the portfolio.

CONSOLIDATING THE PORTFOLIO

Identifying the situation

One of the key issues brand owners must address is the decentralized nature in which domain names may be handled internally. Historically, different domain name providers and different departments may have been involved in registering and managing domains, resulting in a fragmented portfolio.

In order to consolidate domain names, companies must first identify:

- Where they are currently registered
- Registrations carried by authorized partners (such as licensees)
- Industries such as fashion may have particularly complex licensee structures
- Third party domain names, including potentially infringing names
- If domain names adhere to standard registration details

Centralizing and standardizing registrations

Without a centralized portfolio and standardized information, keeping track of renewals and new registrations can be problematic. Renewal applications, payment details and a variety of administrative tasks may be dispersed across different providers or business units, resulting in mistakes. In particular, renewal notices may be sent to the incorrect contact and cause administrative problems. A consolidated portfolio will:

- Enhance administrative and budgetary control
- Increase the effectiveness of registration and renewals management
- Allow centralized or decentralized billing and approval processes within a company

To do this, companies should consolidate all registrations with one domain name provider. This will enable the provider to then:

- Implement an online domain name management solution that enables the consolidation, registration and maintenance of the portfolio
- Perform registrant transfers to correct domain name information if required
- Advise on and implement best practice for domain name registration templates
- Carry out domain name modifications to change contact information, name servers and registrant information accordingly

DEFINING INTERNAL PAYMENT STRUCTURES AND POLICIES

Payment will depend on two factors:

- Is the budget centralized or decentralized?
- Is the approval of invoices centralized or decentralized?

Therefore, there are four general payment models to select from.

1) Centralized budget with centralized approval

Under this option, both the budget and approval may be centralized with the global head office, and little or no involvement is required from any regional offices.

2) Centralized budget with decentralized approval

In this case, while the budget is centralized, the actual approval of invoices may be carried out by regional offices who carried out the registration orders. This option would require careful co-ordination between the offices as the invoices would be sent to the head office and be farmed out to the regional offices for signature.

3) Decentralized budget with centralized approval

A reverse of option 1, in this case the regional offices would hold individual budgets for their territories, but payment must be authorized by the central office.

4) Decentralized budget with decentralized approval

Here, invoice approval would be carried out by a number of different offices. It may be that each regional office receives, approves and pays their own invoices relating to their territories.

MONITORING THIRD PARTY REGISTRATIONS

Registering brands in every permutation of a name in every TLD is often not a cost-effective strategy. As such, protecting an online identity is an ongoing operation that requires effective and regular monitoring tactics, as well as a strategy on how to tackle potential infringements.

Monitoring

New domain name registrations are continuously implemented on the Internet. Therefore, keeping informed of those domain names that could infringe company's brands is a continuous and time-consuming task.

Third-party solutions can help. CSC Corporate Domains provides a Domain Name Watching service; a monthly monitoring service to inform clients of new registrations containing their trademarks, including variations such as "brandsucks.com".

TRACKING AND REPORTING

A domain name policy should incorporate mechanisms to monitor that it is being correctly implemented and to keep those involved informed of progress.

Often, this is most effectively done through online portfolio management solutions such as Name Console 2.0 from CSC Corporate Domains. Name Console 2.0 allows client-specific access rights. Therefore, users can create their own "workgroup" profiles, giving them control over which users can access which functional and reporting modules.

Business unit tracking

Where a company's domain name strategy encompasses different business units – whether they relate to different brands and business divisions – Name Console 2.0 can be configured to incorporate these structures. This includes restricting user-access, where required, by business unit, and grouping orders by business unit on invoices. In doing so, companies can track and manage activity more effectively across the global offices.

Order status tracking

To support the interaction between clients and CSC Corporate Domains fulfillment and account management teams, Name Console 2.0 provides:

- A home page summary of order statuses including orders awaiting approval and "on hold", plus an optional scheduled weekly email summary
- Real-time information on order status details
- An optional email alert when orders are completed, rejected or placed "on hold"

Part 2 – Developing a Domain Name Strategy

DEFINING KEY BRANDS AND TERRITORIES

When developing a domain name strategy, one of the first requirements of a company is to identify their key brands and territories. This may be determined through input from both marketing and legal strategies.

- A marketing strategy could determine key brands and territories as they relate to revenue-generation, local markets and brand awareness

- A legal strategy could determine the brands and territories that require the greatest protection from infringement.

Once these are identified, they should be reviewed in terms of the online world. Under the ccTLDs, there are over 1500 possible domain name extensions in which to register. Even a single name in each of the jurisdictions that accept public registration would cost businesses a five-figure sum per year. In order to register name variations, adding in associated professional fees, the annual budget rises into six figures.

So where should companies register brands for which the budget is more limited?

Learning from traditional brand protection, it might be tempting to register only in those countries where the company does business or expects to trade in the future. While these territories should form the first aspect of a registration strategy, relying on these alone may not be appropriate online. Names registered in the smallest Pacific islands are accessible worldwide. Furthermore, many ccTLDs have departed from the idea of representing their host countries at all. Tuvalu – home of the .tv domain name – is probably the best known of these 'commercialized' ccTLDs.

In additional to registering according to geographical markets, companies should base decisions both on how likely it is that an infringement will occur, and on how hard it is to deal with if it does.

Restricted and unrestricted territories

Famous brands are a common target for cybersquatters who can register brands or trademarks as domain names to be used in bad faith. Although most infringements take place in .com due to the low registration fees and the easy registration requirements, many ccTLDs are nearly as easy to register and therefore are a target for cybersquatters.

The ccTLDs can be classified into 3 categories:

Unrestricted: These have few or no restrictions to registering a domain name. The freedom offered by the unrestricted ccTLDs may enable corporations to easily secure a domain name where, for example, they may not have a local company - often a requirement of registering certain country-code domain names - or when the corporation wishes to register a domain that is not identical to its trademark. However, by the same token, companies' brands are at a greater risk of being registered by third parties, opening up the possibility to cybersquatting in these markets.

Semi-restricted: These have some restrictive rules that, for example, require applicants to be a locally registered company. Here, the risk of cybersquatting is less, but still present.

Restricted: These are the most restrictive of the classifications, where the potential for cybersquatting is at its least. They have varying forms of restrictions and provide fewer concerns for trademark owners as they create additional challenges for potential cybersquatters. However, companies wishing to utilize a local online presence may also be prevented from doing so if they do not meet the criteria of the registry.

Availability of dispute resolution and litigation

Another influencing factor is how easy it would be to reclaim an infringing name. The Internet Corporation for Assigned Names and Numbers' (ICANN) Uniform Domain Name Dispute Resolution Policy (UDRP) has made it easier for brand owners to tackle clear-cut cases of cybersquatting.

However, there remain many territories that are not covered by a dispute resolution policy. Here, often the only legal action available to reclaim a name is litigation and, notably, not all jurisdictions have developed their trademark laws to include domain name infringement.

Often dispute resolution, legal action or out of court negotiations do not succeed in securing the transfer of a third party name. In these instances, the choice is whether to accept the loss or purchase the domain name registration.

With so many factors governing companies' decisions on where to register, choices should firstly be based on the reach of the brand. While it may be best to compromise in the restricted territories, it is wise to ensure a variety of domains are covered, including variations, in the major gTLDs and all brands in the unrestricted jurisdictions.

A tiered domain name strategy

The basis of a tiered approach is registering names in locations where the company does business and where products are sold, as well as higher risk extensions for top trademarks. The first step is defining the company's brands, their value in relation to each other, and the markets in which they are sold.

TIER 1 – HOUSE BRANDS ONLY (CORPORATE); REGISTERED AS DOMAIN NAMES IN COUNTRIES WHERE THE COMPANY OR ITS AFFILIATES DO BUSINESS.

Suggested approach:

- The domain extensions should include top-levels and second-levels, e.g. mycompany.ro, mycompany.co.ro and mycompany.com.ro.
- A maximum of three domains per mark, per country should be registered.
- The major brands should also be registered across all gTLDs and high-risk ccTLDs, as detailed above, where the company may not conduct business/
- In addition, these top marks should be defensively secured in all new gTLDs, such as .pro and .name.

TIER 2 – PRODUCTS ONLY (COMMERCIAL TO REVENUE); REGISTERED AS DOMAIN NAMES WHERE PRODUCTS ARE SOLD AND IN HIGH-RISK COUNTRIES.

Suggested approach:

- A maximum of two country code domain names per mark per country on the top-level and second-level.
- gTLDs should also be secured.

TIER 3 – OTHER BRANDS (MARKS TO MARKET); REGISTERED ONLY WHERE BRAND OR NAME IS MARKETING.

Suggested approach:

- Secure the top-level extensions only.
- A maximum of one per country such as "brand.fr".
- gTLDs should also be secured.

TIER 4 – ALL OTHERS; INCLUDES MISSPELLINGS, UNIQUE SPELLINGS, PROGRAMS, PROMOTIONS OR MISCELLANEOUS DOMAIN NAMES. IN ADDITION, ALL DOMAIN NAMES THAT ARE REQUESTED BY BUSINESS UNITS THAT DO NOT CORRESPOND TO A TIER 1-3 SHOULD BE TAGGED AS TIER 4.

Suggested approach:

- Register in gTLDs and a maximum of two domains per mark per country as necessary.

A tiered approach can help protect a company's brands in a cost effective manner, while also providing the framework for ad hoc domain name requests. It will also help avoid costs to recover domain names and ensure that those domain names are available for use by the company and affiliates, when needed. Such a strategy may lead to long-term savings and a greater online experience.

Managing Non-English Language Domain Names

As part of ongoing efforts to reach a truly global online audience, Internationalized Domain Names (IDNs), or non-English language domains, is a global trend and becoming increasingly popular for registries to offer and for companies to include in their domain name portfolios. An IDN is a domain name that uses characters outside of the English alphabet, such as æ, ü and é, known as non-ASCII characters. These can also include Asian, Hebrew and Arabic characters.

The Internet Engineering Task Force (IETF) now has introduced a standard protocol for dealing with IDNs within the domain name system. The standards use an ASCII-compatible encoding (ACE) known as "punycode" which enables domain names with non-English alphabet characters to be converted into ASCII.

IDNs do not currently resolve on the Internet in the standard manner. If end users input non-Latin alphabet characters as part of a domain name or if a web page contains a link using non-Latin characters, the application must convert this from its native string into a special encoded format (i.e. punycode) using only the usual ASCII characters. However, not all applications have this functionality.

For a user to view a website attached to an IDN, there are currently two solutions which enable many IDNs to be viewed. One is to use a plug-in, which is provided by some registries such as VeriSign. The other option is to use a browser that is equipped to handle IDN domain names. Some native browsers, such as in China, currently have this capability.

IDNs are still not accessible to most Internet users. They do not, and may never, have the same functionality as traditional ASCII domain names. We do not know if or when increased functionality will be available from the IDN registries. Register.com is offering this service to clients to help protect their domain names in the event these names become functional on the Internet.

MANAGING BUSINESS CHANGES AND DEVELOPMENTS

A number of business changes require forward planning when it comes to integrating them with the domain name strategy. Of particular note are:

• Launch of new brands and products

• Rebranding exercises

• Mergers and acquisitions

In each of these cases, there is a requirement for additional domain name registrations to both protect these brands from third party use and to enable future website launches for marketing purposes.

Key to ensuring this is planned and implemented successfully is the integration of marketing and legal departments.

When a new brand is involved, companies not only have to think about traditional branding but also about how they want to market themselves on the web. A consistent message across all media is the key. In the first instance, that means ensuring that the different elements of a brand can be protected as trademarks and other forms of intellectual property, and also that it is possible to secure domain name registrations in all relevant markets, which it may not be.

Therefore, it is important for marketers to understand that prompt domain name searches can save an awful lot of time and money further down the line, and that these are best done by the experts, not in an ad hoc manner through simple Internet searches.

Beyond searching, however, there are other issues to consider. As trademark lawyers know, domain names and trademarks are not necessarily the same, and what can be registered and protected for use online will often

cause problems as a traditional trademark. By choosing descriptive domain names, registrants are limiting their ability to operate in the future.

Marketers may view trademark practitioners as obstructive to their requests, and the lawyers may regret that they get involved too late in the branding process, or, in some cases, are ignored altogether. It is a fact which many companies recognize.

However, the two can work together successfully when there is a properly organized process that allows them to do so. This is clearly demonstrated by the rebranding exercise undertaken by KPMG Consulting Inc when it became BearingPoint Inc in October 2002. The job allocated to a joint marketing and legal team was to pick a new name and then ensure a simultaneous change to this on all company literature, websites, signs and other forms of distinguishing material to coincide with a switch of listing from Nasdaq to the New York Stock Exchange. What made it harder was that they were given only 90 days in which to do the job, as opposed to the 9 to 12 months such a task commonly takes.

An initial list of 550 company names was quickly whittled down to 100, with 90 more ruled out by the lawyers by mid-August. Once BearingPoint had been agreed, trademark and domain name registrations had to be secured in 134 countries, and they were[1]. Such an outcome would not have been possible without centralized management.

This coordination between different departments is not just relevant in terms of business changes, it should also echo through the whole domain name strategy.

MANAGING DOMAIN NAME INDUSTRY DEVELOPMENTS AND CHALLENGES

Each company will have a strategy that is unique to them. However, all strategies should have the flexibility and provisions to address the frequent and sometimes significant changes in the domain name market. These may include:

- The launch of new gTLDs and ccTLDs
- The creation of new second-level extensions within an existing TLD, e.g. .kids.us
- The liberalization of ccTLDs
- Internationalized domain names

For each of these opportunities there should be clear policies on how the company will respond. Some strategies will dictate that all new gTLDs and ccTLDs should be covered. Others will require registrations only in those that match the criteria previously set out, for example only unrestricted ccTLDs and territories in which the company is trading.

TACKLING THIRD PARTY DOMAIN NAME REGISTRATIONS

Taking Action

Some companies will take a harsh line on challenging any third party registration which contains its trademarks or variations thereof. For many, this is the most appropriate method of enforcing their IP rights and protecting their brands online. However, some choose a more lenient approach. Often, overly enforcing IP rights may result in negative PR. Whichever the approach, companies may need to decide on a case-by-case basis.

Before proceeding with any action to reclaim a domain name, companies need to ensure they are adequately prepared.

Domain Name Investigations

The first step to recovering a domain name is to carry out an investigation that will determine what rights the trademark owner has to the name and further details of the registrant. One problem with domain disputes is that tracking down the person or organization behind the domain name can be difficult. Whois information is fragmented and registrants can use a number of tactics to obscure their identities, such as submitting false or incomplete information to the registry.

Atlantic Coast of America Corporation Ltd v Steven Zaharakis dba Zahara Labs

This case illustrates the importance of a thorough investigation and preparation prior to proceeding with a recovery tactic such as the UDRP. The WIPO Panel noted: "The case is characterised by an extraordinary paucity of information and coherent submission from complainant, and for that matter, from respondent also." Although the Panel agreed that the domain name swreg.com was confusingly similar to Atlantic's trademark, the company had not proved that Zahara Labs was not entitled to use the domain or that it was acting in bad faith. The case was dismissed.

John Ode v. Intership Ltd

If trademark owners invoke the UDRP without having first carried out a detailed investigation, then they could be making a big mistake. An alarming number of UDRP complaints are thrown out due to very simple errors. In this case, the Panel found that the complainant's trading name didn't even exist when the disputed domain was registered.

Once the trademark owner has investigated a domain registrant, discovered his or her identity and built up a pattern of behavior, the next step is to begin the recovery process. Where the UDRP, or a variation, does not apply, negotiation or litigation will most likely be required – however, different approaches are needed in different areas. Not all jurisdictions have developed their trademark laws to include domain name infringement or cybersquatting.

British Telecommunications plc v. One in a Million Ltd

This case is a leading precedent on cybersquatting under English law. In this case the law of passing off was used, for which one of the requirements is to prove misrepresentation that causes actual damage to the business of the trader by whom the action is brought. In terms of domain names, this is difficult to prove from a 'blocking registration' alone. The Court of Appeal ruled that the mere adoption of a trading name can give rise to a misrepresentation that the trade is, in fact, another trader or is in some way connected to that other trader.

US Law

In the US, the courts initially dealt with cybersquatting and other forms of online trademark infringement using the US laws of trademark infringement, unfair competition and trademark dilution. Like English Law, it was generally required that cybersquatters were shown to have sold or advertised some form of goods or services. However, the introduction of the US Anticybersquatting Consumer Protection Act (ACPA) in November 1999 served to strengthen the rights of US trademark owners online by allowing a 'blocking registration' of a domain name to be challenged.

MAXIMIZING USE OF REGISTRATIONS

Companies who maximize registrations are making the Internet work for them, rather than the other way around. In addition to ensuring key brands are protected or represented in key territories and that there

is a strategy for tackling infringements, tactics are deployed to ensure maximum revenue or commercial opportunities. These include:

Making the most of the TLDs

Registrations across the ccTLDs are a valuable method of reaching important local markets. Words associated with your brand can also help drive more traffic. For example, Snapple has registered thebeststuffonearth.com, and Barnes & Noble has registered books.com.

Some extensions provide a creative way of presenting brands. For example, .info is often associated with brochureware, and.biz may be used for specific e-business activities.

In addition, local domain name registrations should point to a live site as a minimum. If defensive registrations are implemented, companies should ensure these are used to harness traffic – if companies are going to register a domain name, they might as well set it up to point to a live site, otherwise it may be a wasted opportunity.

Monitoring Trends

Tracking and monitoring web usage and trends can be invaluable when it comes to making the most of an online presence. Companies should track where traffic comes from as traffic trends in local markets may influence local sites. For example, a high volume of traffic in Germany may indicate a need for further development of a local presence in Germany.

HELPING MAXIMIZE COMPETENCES

Developing Best Practice Through Outsourcing and Consultancy

CSC Corporate Domains is a leading authority for online brand protection and domain name management. Our team of experts are dedicated to registering, managing and monitoring domain names and intellectual property globally on the Internet. By providing assistance with strategic requirements and top-level client service, you can remain in constant control of your online identity and brands.

Our proactive approach has resulted in many of the world's leading brand owners choosing CSC Corporate Domains to manage their brands online. Leading companies, brand managers, IP lawyers, IT and e-commerce professionals from across the globe have recognized our ability to provide solutions to their complex online requirements.

CSC Corporate Domains offers Name Console 2.0, the latest version of the online domain name management solution. Name Console 2.0 incorporates years of experience working with multinational corporate clients and the numerous gTLD and ccTLD registries worldwide.

Name Console 2.0 incorporates a full online order-entry and qualification process, which enables all domain name orders to be raised online. This includes registrations, renewals and modifications under gTLDs and ccTLDs, as well as DNS management services. The solution is:

- Fully customizable to the domain name industry
- Configurable to suit your needs
- Able to develop with your requirements
- Incorporating increased automation to improve speed

Keeping Informed

To ensure both the domain name strategy and policy are up-to-date and implemented effectively, an efficient communications and training programme is required that encompasses all relevant offices and individuals.

Intranets: This is a key way to communicate the strategy across the entire company and can be used to educate, inform and update. Information about the need for global domain name portfolio management and the specifics of company policies may be beneficial to include.

External Resources: There are a number of resources from domain name providers, such as CSC Corporate Domains, to educate on current industry issues and inform companies' strategies. CSC Corporate Domains provides the following free resources:

- • **IP Scan** – an offline magazine containing news, analysis and features about topical online brand management issues.
- • **TLD Update Web site** – an online resource for clients to keep informed of changes in domain name registration rules. Regular email alerts are also sent to flag up forthcoming opportunities.

For more information on domain name policy and strategies, please contact CSC Corporate Domains at:

North America
1133 Avenue of the Americas
Suite 3100
New York, NY 10036

Telephone: +1 800 699 9638
Fax: +1 212 299 5656

Europe
Elysium Gate
126-128 New Kings Road
London SW6 4LZ

Telephone: +44 (0)20 7565 4090
Fax: +44 (0)20 7565 4099

About CSC Corporate Domains

CSC Corporate Domains, Inc. is a wholly-owned subsidiary of Corporation Service Company (CSC). CSC, a privately-held company headquartered in Wilmington, Delaware, USA, is a leading provider of legal, IT and financial services for many of the world's largest companies, law firms and financial institutions. Founded in 1899, CSC, an ICANN accredited registrar exclusively serving global corporations and law firms, is now the largest provider of corporate domain management services. CSC offers clients an integrated, comprehensive portfolio of services that also includes corporate compliance and governance services, entity management services, public record document and retrieval services, uniform commercial code and motor vehicle titling services, litigation management and registered agent services. To learn more about CSC, visit the company website www.incspot.com.

(Footnotes)

[1] http://www.law.com/servlet/contentserver?pagename=openmarket/xcelerate/view&c=lawarticle&cid=103905 453995&t=lawarticleIP