WHITE PAPER

Seven Keys for Successful Domain Portfolio Management

Table of Contents

Executive Summary 3

The Seven Keys for Successful Domain Portfolio Management 4

Key 1: Determine Corporate Objectives for Domain Management 5

Key 2: Adopt Enterprise-Wide Policies and Procedures 7

Key 3: Work with Corporate Subsidiaries and Divisions to Consolidate Domain Names 8

Key 4: Do Not Underestimate the Importance of Registering ccTLDs 10

Key 5: Take Steps to Secure and Protect Valuable Domains 11

Key 6: Implement a Domain Policing Strategy 11

Key 7: Recover Names Using Both Non-Traditional Approaches and Legal Methods 13

Conclusion 16

Executive Summary

The world of domains continues to change at an alarming pace. In the last several years, there has been a proliferation of new top-level internationalized domain names (IDNs), many new second-level and third-level country code top-level domain (ccTLD) offerings, not to mention the launch of hundreds of new generic top-level domains, as part of ICANN's New gTLD Program.

For companies with a global presence, managing an international domain name portfolio has become an increasingly complex challenge and administrators are forced to make important daily decisions about where, when and how to register domain names.

Although domain names are often managed in a manner similar to trademarks, the complexities associated with domain names are far more intricate. Unlike trademarks, domain name restrictions and requirements change rapidly, often making it difficult to stay abreast of these occurrences.

Simply put, without a defined set of guidelines, a clear corporate domain strategy cannot exist. In order to provide guidance to those managing domain portfolios, this document is designed to provide a practical approach to registering and protecting the corporate asset of domain names.

The Seven Keys for Successful Domain Portfolio Management

1. Determine corporate objectives for domain management
2. Adopt enterprise-wide policies and procedures
3. Work with corporate subsidiaries and divisions to consolidate domain names
4. Do not underestimate the importance of registering ccTLDs and IDNs
5. Take steps to secure and protect valuable domains
6. Implement a domain policing strategy
7. Recover names using both non-traditional approaches and legal methods

Key 1: Determine Corporate Objectives for Domain Management

Direction on how to build, maintain and protect a domain portfolio may come from Marketing, Sales, or even the Board of Directors — depending on the type of business and the company's requirements for online exposure or protection.

For example, online retailers often feel compelled to register their key brands worldwide — regardless of where they conduct business — because their domain names are so integral to their ongoing operations. Conversely, a brick and mortar retailer may decide that it is only important to register their brands as domains in countries where they currently conduct business. In essence, there are two different domain registration strategies. There is a Brand Protection Strategy and a Brand Promotion Strategy. Many companies use a combination of the two.

> *There is a Brand Protection Strategy and a Brand Promotion Strategy. Many companies use a combination of the two.*

Brand Protection Strategy

For companies who are concerned about brand abuse and trademark dilution, the Brand Protection Strategy usually makes the most sense. This strategy can be implemented by:

- Registering popular legacy TLDs — .com .net .org .biz .info
- Registering low-cost ccTLDs that are unrestricted or have minimal requirements
- Blocking or registering unrestricted, generic new gTLDs
- Only registering likely targets of domain abuse:
  - Famous Brands
  - Trademarks
  - Slogans
  - "Sucks" sites
  - Singular and plural
  - Common misspellings, including IDNs

Brand Promotion Strategy

For companies who are concerned with worldwide brand promotion, portraying a sense of cultural understanding, and increasing Internet-generated revenue, the Brand Promotion Strategy usually makes the most sense. This strategy is characterized by:

- Registering in geographic locations where you have offices or do business
- Registering all legacy gTLDs
- Registering select new gTLDs
- Focusing on top ccTLD extensions
- Focusing on top e-commerce countries
- Registering multiple variations
- Trademarks
- Slogans
- Singular and plural
- Common misspellings
- Brand and Product type (www.banknamemortgage.com)
- IDNs
- Register third-level name to gain first rights to second-level names

Many companies use a combination of both strategies for managing their domain portfolio, depending on the brands that they are registering.

When devising a strategy, also take into consideration new names that your company may want to use in the future, different geographical regions in which you are doing business, or geographical regions where you may consider doing business in the future. Remember of course, that many countries have restrictions such as local presence requirements, which must be satisfied in order to register in those regions.

Two Approaches to Domain Management

1. Brand Protection
   - Focus on low-cost, unrestricted extensions
   - Align with trademark registrations
   - Anticipate future marketing needs
   - Famous house brand protected everywhere
2. Brand Promotion
   - Maximize corporate exposure on the Internet
   - Top 10, 25, or 50 e-commerce countries
   - Generate e-commerce revenue worldwide
   - Support worldwide sales and marketing efforts

600+

The number of open new gTLDs added to the domain landscape.

Key 2: Adopt Enterprise-wide Policies and Procedures

As changes to ccTLDs can happen quickly and with more than 600 open new gTLDs added to the domain landscape, it is especially important to create enterprise-wide policies and procedures covering who can register domains, and how they will be registered.[1] In particular, it is important to identify the individuals who are permitted to request, approve and modify registrations. If more than one person is granted the ability to make changes, it is still advised that a central point of contact is tasked to review and approve all orders.

It is also important to determine a preferred Administrative Contact. This Administrative Contact, which appears on the domain ownership record (also known as the Whois record), is generally the recipient of renewal and expiration notices. Consequently, problems can arise if an individual's information is used when that employee leaves the company and their email accounts are deactivated. Also, unauthorized transfers can occur if emails are not monitored. By using a company-controlled email alias such as admin@yourcompany.com, these problems can be diverted, by ensuring that someone is always available to review and respond to important registrar communication.

Determining where you want your domain names to point is another critical decision which should be addressed. For example, if an Internet user types in one of your domain names, where do you want that user to go? Should it resolve to a main corporate site, an e-commerce site or an HR site? Many companies match foreign-language domain names (IDNs) to language-specific websites.

Keeping a list of brands to be registered regardless of geographic location can also decrease the likelihood that a name will be lost to a cybersquatter. This is especially true given that many new ccTLD offerings are announced and made available with very little notice.

Using a Reverse Whois tool provides one method for uncovering domains that belong to your organization.

Another policy to be implemented revolves around the locking of domain names. By locking a domain name, unauthorized transfer or changes to the DNS cannot be made.

The last policy that should be addressed is related to domains that are lost as the result of unintended expiration, domain hijacking or cybersquatting. Having a plan to respond to these situations can greatly reduce corporate exposure and expense. A successful plan should minimize damage to customer data as well as curtail reputational damage to the company. To accomplish this, different organizational departments may need to respond including:

- Public Relations – To respond to media inquiries regarding the event
- Legal – Both inside and outside counsel to determine the best course of action
- Customer Service and Marketing – To notify and inform customers of potential scams

Key 3: Work with Corporate Subsidiaries and Divisions to Consolidate Domain Names

Consolidating a corporate domain portfolio begins with identifying all of the domain names and variations registered for your company and its products, services, trademarks, and brands. Once these domains have been identified, they should be consolidated into a single repository for further review.

While this may seem like a fairly simple task, doing so may actually be quite cumbersome due to the fact that various departments and subsidiaries may have registered domain names directly at some point in the past.

Using a Reverse Whois tool provides one method for uncovering domains that belong to your organization. Reverse Whois tools enable the identification of domain names by searching for any term

"After domains have been identified, managing and monitoring them in an online repository is key."

within a Whois record including: contact, company, email, address, and name server.

Contacting likely registrants is another method for uncovering domain names. Likely registrants of domains include: marketing managers, web administrators, product managers and legal.

By consolidating domain portfolios, domain administrators can:

- Gain visibility into their entire portfolio
- Work with a single registrar who understands their company's corporate objectives
- Compare trademark registrations against all existing domain registrations to identify gaps
- Reduce the costs of working with multiple registrars

After all domains are uncovered, it is important to review each domain name to ensure that they meet established standards, and that contact information has been updated for each name. If there are inconsistencies, Whois modifications should be made as quickly as possible for all gTLDs to meet ICANN requirements. In cases where there are ccTLD inaccuracies, and where special requirements exist, perform necessary modifications to reflect as much consistent contact information as possible.

After domains have been identified, managing and monitoring them in an online repository is key. When selecting an online repository, it is critical that the application provides:

- Ability to track and manage domains for multiple users and subsidiaries
- Highly detailed and flexible billing
- Ability to assign different user privileges
- Bulk registration and edit capabilities
- Auto-renew functionality
- Flexible sorting and filtering
- Configurable interface

Key 4: Do Not Underestimate the Importance of Registering ccTLDs and IDNs

Although in the United States .com and .net are the most sought after extensions, in other parts of the world, particularly Europe and Asia, ccTLDs reign supreme. Of the 330.6 million domain names currently registered, more than 143 million are ccTLDs. This represents 43% of all domain name registrations. Moreover, ccTLDs continue to grow and have risen 3.1% in the last year alone.[2]

One reason for this is that countries, in recognizing revenue potential, are continuously changing their rules, and removing restrictions from registrations to increase their numbers. In addition to decreasing their requirements, ccTLD registries are also barraging the market with new second-level and third-level offerings. For example, in 2015, .IN (India) announced 12 new second and third level offerings. That said, it is important to note that the top ten ccTLD registries comprise 64.7% of all ccTLD registrations. Consequently, the need to continually monitor ccTLD registry changes exists.[2]

Unfortunately, the popularity of ccTLDs has led to predatory practices and abusive and bad-faith registrations of protected names. Because each ccTLD administrator sets its own policy for selling, operating, and managing Internet addresses within its proprietary domain, trademark owners often have a difficult time enforcing their rights.

When selecting a registrar be sure to recognize that many can provide complete ccTLD capabilities including local presence services and local contact services — making it easier to qualify for registration.

The Top10 ccTLDs

1. .cn (China)
2. .tk (Tokelau)
3. .de (Germany)
4. .uk (United Kingdom)
5. .ru (Russian Federation)
6. .nl (Netherlands)
7. .br (Brazil)
8. .eu (European Union)
9. .au (Australia)
10. .it (Italy)

As of March 31, 2016[2]

Key 5: Take Steps to Secure and Protect Valuable Domains

Undoubtedly, some domains are more valuable than others. Clearly, domains that point to high traffic sites, corporate websites and e-commerce sites are more valuable than those registered in an effort to protect against cybersquatting or typo squatting.

For highly-valued domains, it is recommended that special care be taken. Specifically, these domains should be registered for the maximum allowable term; for gTLDs this is ten years. These domains should also be locked at the registry level to protect against unauthorized domain transfers (hijacking). Of course, domains that are highly valued should be set to automatically renew each year, and most domain registration portals provide this functionality.

As previously mentioned, using a company-controlled email alias such as admin@yourcompany.com for the Administrative Contact on Whois records is critical. This ensures that someone is always available to review and respond to important registrar communications.

And finally, ensuring accuracy of Whois data is critical as ICANN mandates that the provision of false or incorrect Whois information can be grounds for cancellation of the registration.

Key 6: Implement a Domain Policing Strategy

Implementing both a Brand Protection Strategy and a Brand Promotion Strategy can provide extensive coverage. However, registering every possible domain name in every single country, and in every new top level extension, is simply not a practical solution.

Cybersquatters and phishers continue to redirect Internet traffic to fraudulent websites by registering domains that are confusingly similar to legitimate sites. Stolen business, angry customers, damaged reputations and legal battles are just some of the problems that can ensue if preemptive measures are not taken.

Registering domains should be viewed as a first line of defense against brand abuse. Monitoring

Protect Valuable Domains

- Register domains for maximum allowable terms
- Lock domains at the registry level
- Utilize company controlled email aliases
- Ensure accuracy of Whois data

domain name registrations of others provides a second line of defense.

Domain name monitoring can be accomplished by searching through zone files for newly added domain names that contain a particular search term. There are a number of services available that can provide this information on a daily basis.

Important features of a domain name monitoring service include:

- Notification of newly registered domains and newly dropped domains
- The ability to create exclusion lists and search zone files using wildcards
- The status of each reported domain (active/inactive/dropped)
- A live link for each domain
- A live link to the Whois record for each domain

By monitoring domain registrations, companies can proactively anticipatepotential domain name abuse and take immediate action. This can include actively monitoring a site, filing a UDRP action or challenging the accuracy of the Whois record, if the name falls into the hands of a suspicious individual or entity.

In addition to fraudulent activities that require monitoring, there are a number of legitimate business activities, which should be reviewed as well. These events include:

- Mergers and acquisitions
- Deployment of new product or service development
- Market development or introduction of products and services into a specific country
- New servers or security arrangements
- Transfer or termination of key employees
- Address changes

Key 7: Recover Names Using Both Non-Traditional Approaches and Legal Methods

Even the best-managed domain portfolios can be the target of cybersquatters or phishers. As mentioned previously, registering every possible domain name in every single country and new top level extension is not a practical solution. As a result of monitoring the domain registrations of others, it may become apparent that some lost domains need to be reacquired immediately. In determining how to reacquire lost domains, keep in mind that there are both legal approaches and non-traditional methods available.

Non-Traditional Approaches

Reacquiring domains through anonymous acquisition is often preferable if UDRP or legal proceedings (and related publicity) are unattractive or inappropriate, and expeditious recovery is required. A third party who offers domain acquisition services may be able to acquire the domain at a significantly reduced rate.

If Whois content is inaccurate or fraudulent, it may also be possible to quickly recover names. To expedite this process, notification of fraudulent Whois records must be submitted to ICANN at http://wdprs.internic.net/

If time is not a concern, another approach is to monitor expiration dates, and to register the name should it become available. This approach should only be used if the name is a "nice to have" as opposed to a "must have."

Traditional Approaches and Legal Methods

Uniform Dispute Resolution Policy (UDRP)

One of the most common approaches for reacquiring domains is through ICANN's Uniform Dispute Resolution Policy (UDRP). Eighty-nine percent of all UDRP cases are held in favor of the trademark holder and the fees and costs are typically less than $10,000.[3] The average time to resolution is approximately eight weeks. As a result anonymous acquisition makes more sense in many cases.

To win a UDRP, the Complainant must prove that the domain name is identical or confusingly similar to a trademark or service mark in which the Complainant has rights. Although trademark registration is not required, it is helpful. It must also be proven that the registrant has no rights or legitimate interest in the name.

Finally, bad faith registration and use must be shown. Use can be established with attempts to sell, routing to adult sites, or using the domain name to draw traffic meant for Complainant's site.

Anti-Cybersquatting Protection Act (ACPA)

The Anti-Cybersquatting Protection Act (ACPA) is a U.S. law designed to prohibit cybersquatting, including: extracting ransoms from trademark

holders for names; offering domain names for sale to the public; diversion of customers to pornographic sites; warehousing domain names of well-known trademarks and engaging in acts of consumer fraud.

Temporary restraining orders are available based upon the ACPA and can be achieved more quickly than the resolution of a UDRP proceeding.

Under the ACPA, statutory damages of $1,000-$100,000 per infringing domain name and attorney's fees are recoverable.[4]

The Digital Millennium Copyright Act (DMCA) protects Internet service providers (ISPs) with a safe-harbor if the ISP: designates an agent to receive notifications of infringement; develops a proper notification procedure; and develops take down procedures.

Trademark holders invoking the DMCA should send a notice of copyright infringement in conformance with the Act addressed to the ISP's designated agent which: identifies and describes the infringed copyrighted works; provides

a clear description of where the infringing material is located; contains complainant contact information; and is signed under penalty of perjury. Results under the DMCA are frequently expeditious.

New gTLD Rights Protection Mechanisms

Additionally, as part of the new gTLD Program, ICANN has adopted a number of New Rights Protection Mechanisms designed to protect brand owners.

Uniform Rapid Suspension (URS) System

All new gTLDs will be subject to the URS system. The URS system is designed to provide a cost-effective, expedited process to address issues of trademark infringement and abuse. Form complaints are filed electronically and are designed to be as simple and formulaic as possible. The complainant may submit no more than 500 words of explanatory free-form text

and fees are $375 per filing, consisting of up to 14 domains.[5] Domains are only suspended for the remainder of their registration term, or for an additional year at current market registration rates. After suspension ends however, domains become available for registration and may be registered again resulting in a never-ending cycle of watching and suspending.

Post-Delegation Dispute Resolution Procedure (PDDRP)

The PDDRP will also provide rights holders with the ability to file complaints against registries who have acted in bad faith with the intent to profit from the systematic registration of infringing domains at the second level (to the left of the dot). According to ICANN, an example of infringement is where a registry operator has a pattern or practice of actively and systematically encouraging registrants to register domain names and to take unfair advantage of the trademark to the extent and degree that bad faith is apparent. Another example of infringement is where a registry operator has a pattern or practice of acting as the registrant or beneficial user of infringing registrations to monetize and profit in bad faith. For infringement occurring at the second level, possible remedies may include requiring the registry to implement measures to protect against allowing future infringing registrations or the suspension of accepting new domain name registrations until violations are cured.

Registry Restriction Dispute Resolution Procedure (RRDRP)

The RRDRP is a complaint procedure for community-based gTLDs in which the complainant asserts that it is "a harmed established institution as a result of the community-based gTLD registry operator not complying with the registration restrictions set out in the Registry Agreement." The complainant must prove that the TLD operator violated the terms of the community-based restrictions in its agreement and that there is measureable harm to the complainant and the community named by the objector.

Conclusion

In the past, corporations struggled with managing global domain name portfolios due to decentralized account management and lack of standardized procedures. This lack of centralization and coordination had resulted in the expiration of domain names, failure to register key domain names, and the loss of domain names to cybersquatters.

Clearly more emphasis is being placed on the management of domains as they are now viewed as important intellectual property. As the industry continues to mature and more new TLDs are launched, the management of large portfolios will likely become increasingly complex. Protecting domains from cybersquatters and phishers will continue to be a priority as many wide-open namespaces have become available with the launch of hundreds of new gTLDs.

Whatever the future may bring for domains, of one thing we can be certain: domain name management is critical for both protecting against brand abuse and trademark dilution, as well as promoting brands to a worldwide audience.

[1] ICANN, "Delegated Strings," https://newgtlds.icann.org/en/program-status/delegated-strings, August 2016.
[2] VeriSign, Domain Name Industry Brief, July 2017.
[3] WIPO, "Schedule of Fees under the UDRP (valid as of December 1, 2002)," http://www.wipo.int/amc/en/domains/fees/index.html, August 2016.
[4]
pdf, November 25, 2013.
[5] ICANN, "URS Request For Information Frequently Asked Questions (FAQs)," https://newgtlds.icann.org/en/applicants/urs/rfi-faqs, August 2016.

About MarkScout

MarkScout provides online brand protection and domain management for global brands. Our technology and experts detect and remove counterfeits, piracy, fraud and brand abuse across marketplaces, social media, domains and the dark web, helping protect revenue, reputation and customer trust. To learn more, visit markscout.com.

LEARN MORE

MARKSCOUT.COM/SERVICES/DOMAIN-MANAGEMENT