

Seven Keys for Successful Domain Portfolio Management

By Elisa Cooper
Director of Product Marketing, MarkMonitor

Abstract

The world of domains continues to change at an alarming pace. In the last several years, there has been a proliferation of new ccTLD IDNs (Internationalized domain names), many new second-level, and third-level ccTLD offerings, nine new sTLDs, significant changes to ICANN's Transfer and Whois Policies, and finally, ICANN's proposal to allow an unlimited number of new gTLDs, including IDN TLDs.

For companies with a global presence, managing an international domain name portfolio has become an increasingly complex challenge. With more than 249 ever-changing ccTLDs, domain 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 large domain portfolios, this document is designed to provide a practical approach to registering and protecting the corporate asset of domain names.

Contents

Overview	3
The Seven Keys for Successful Domain Portfolio Management	3
Key 1: Determine Corporate Objectives for Domain Management	3
Key 2: Adopt Enterprise-Wide Policies and Procedures.....	5
Key 3: Work with Corporate Subsidiaries and Divisions to Consolidate Domain Names	6
Key 4: Do Not Underestimate the Importance of Registering ccTLDs	8
Key 5: Take Steps to Secure and Protect Valuable Domains	8
Key 6: Implement a Domain Policing Strategy	9
Key 7: Recover Names Using both Non-Traditional Approaches and Legal Methods	10
Conclusion	12

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
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

Understanding your company's corporate online objectives is the first step in creating a comprehensive domain portfolio. 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.

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 gTLDs — **.com .net .org .biz .info**
- Registering low-cost ccTLDs that are unrestricted or have minimal requirements — **.at .be .cc .eu .ch .cn .co.uk .dk .it .nl .ru .tv .us .ws**

Without a defined set of guidelines, a clear corporate domain strategy cannot exist.

Two Approaches to Domain Management

1. Brand Protection

- Focus on low-cost, unrestricted extensions
- Anticipated future marketing needs
- Famous "house" brand protected everywhere

2. Brand Promotion

- Maximize corporate exposure on the Internet
- Top 10, 25, or 50 eCommerce countries
- Generate eCommerce revenue worldwide
- Support worldwide sales and marketing efforts

- Only registering likely targets of domain abuse
 - Famous Brands
 - Trademarks
 - Slogans
 - “Sucks sites”
 - “-” for two word names
 - wwwname.com
 - Singular and plural
 - www.myname.com
 - Common misspellings, including Internationalized Domain Names
 - Famous Executives, BODs and Brand + Product type (www.banknamemortgage.com)

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 all gTLDs
- Focusing on top ccTLD extensions — **.ar .asia .at .au .be .br .ca .cc .ch .cn .cz .de .dk .eu .fr .it .jp .kr .nl .no .nu .nz .pl .ru .se .tv .tw .uk .us .ws .za**
- Focusing on top eCommerce countries — **.at .br .ca .co.mx .co.uk .de .fr .jp .it .nl**
- Registering multiple variations
 - Trademarks
 - Slogans
 - “-” for two word names
 - www.wwwname.com
 - Singular and plural
 - www.myname.com
 - Common misspellings
 - Brand + Product type (www.banknamemortgage.com)
 - Internationalized Domain Names
 - 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.

Key 2: Adopt Enterprise-wide Policies and Procedures

As changes to ccTLDs can happen quickly and often without warning, it is especially important to create enterprise-wide policies and procedures covering who can register domains, and how they will be registered. In particular, it is 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.

In addition to setting up role-based 'Administrative Contacts', it is necessary to set standards for how 'Registrant', 'Technical' and 'Billing' data should appear in Whois records. It is critical that this information is accurate per ICANN, the governing body for all gTLD registrations.

It is also important to determine which individuals in the company should be permitted to approve orders for new domain names, renewals, and modifications. 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. This central point of contact can either be 'in-house', or outside intellectual property counsel.

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 eCommerce 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.

Another policy to be implemented revolves around the 'Locking' of domain names. By 'Locking' a domain name, unauthorized transfer or changes to 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:

- PR – To respond to media inquiries regarding the event
- Legal – Both inside and outside counsel to determine the best course of action
- Customer Service/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 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 online 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

Although in the United States .com and .net are by far the most sought after extensions, in other parts of the world, particularly Europe and Asia, ccTLDs reign supreme. Of the 177 million domain names currently registered, more than 71.1 million are ccTLDs. This represents close to 40% of all domain name registrations. Moreover, ccTLDs continue to grow at an alarming rate. Growth rates for ccTLDs have risen 22% in the last year alone.

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 constantly barraging the market with new second-level and third-level offerings. For example, in 2004, .it (Italy) announced 103 new third-level offerings. That said, it is important to note that the top ten ccTLD registries comprise 65% of all ccTLD registrations. Consequently, the need to continually monitor ccTLD registry changes exists.

The Top 10 ccTLDs (as of January 2009):

1. .cn (China)
2. .de (Germany)
3. .uk (United Kingdom)
4. .nl (Netherlands)
5. .eu (European Union)
6. .ar (Argentina)
7. .it (Italy)
8. .br (Brazil)
9. .us (United States)
10. .au (Australia)

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

Unfortunately, the increasing popularity of the 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.

Of the 249 ccTLDs, only 114 have publicly released registration rules and requirements, 19 have a Whois service of which many are poorly maintained, 56 have adopted an Alternative Dispute Resolution (ADR) procedure and 49 ccTLDs do not even have a web presence. Additional information is located at http://arbiter.wipo.int/Domains/cctld_db/index.html.

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.

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 eCommerce 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 communication.

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 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 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 anticipate potential 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 is not a practical solution. As a result of monitoring the

Registering domains is a first line of defense against brand abuse. A second line of defense is monitoring domain name registrations of others.

domain registration 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 of 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

UDRP

One of the most common approaches for reacquiring domains is through ICANN's Uniform Dispute Resolution Policy (UDRP). Eighty-five percent of all UDRP cases are held in favor of the trademark holder and the fees and costs are typically less than \$10,000. 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.

UDRP only applies to gTLDs. Only 23% of all ccTLDs have some type of resolution policy to protect trademark holders.

ACPA

The Anti-Cyber Squatting 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.

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.

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 new gTLDs are launched, the management of large portfolios will likely become even more complex. Protecting domains from cybersquatters and phishers will continue to be a priority as many wide-open namespaces will become available with the expected launch 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.

About MarkMonitor

MarkMonitor, the global leader in enterprise brand protection, offers comprehensive solutions and services that safeguard brands, reputation and revenue from online risks. With end-to-end solutions that address the growing threats of online fraud, brand abuse and unauthorized channels, MarkMonitor enables a secure Internet for businesses and their customers. The company's exclusive access to data combined with its real-time prevention, detection and response capabilities provide wide-ranging protection to the ever-changing online risks faced by brands today.

To learn more about MarkMonitor Domain Management the MarkMonitor Brand Protection Platform and Services, please visit www.markmonitor.com.

More than half the Fortune
100 trust MarkMonitor to
protect their brands online.
See what we can do for you.

MarkMonitor Inc.
U.S. (800) 745.9229
Europe +44 (0) 207.840.1300
www.markmonitor.com