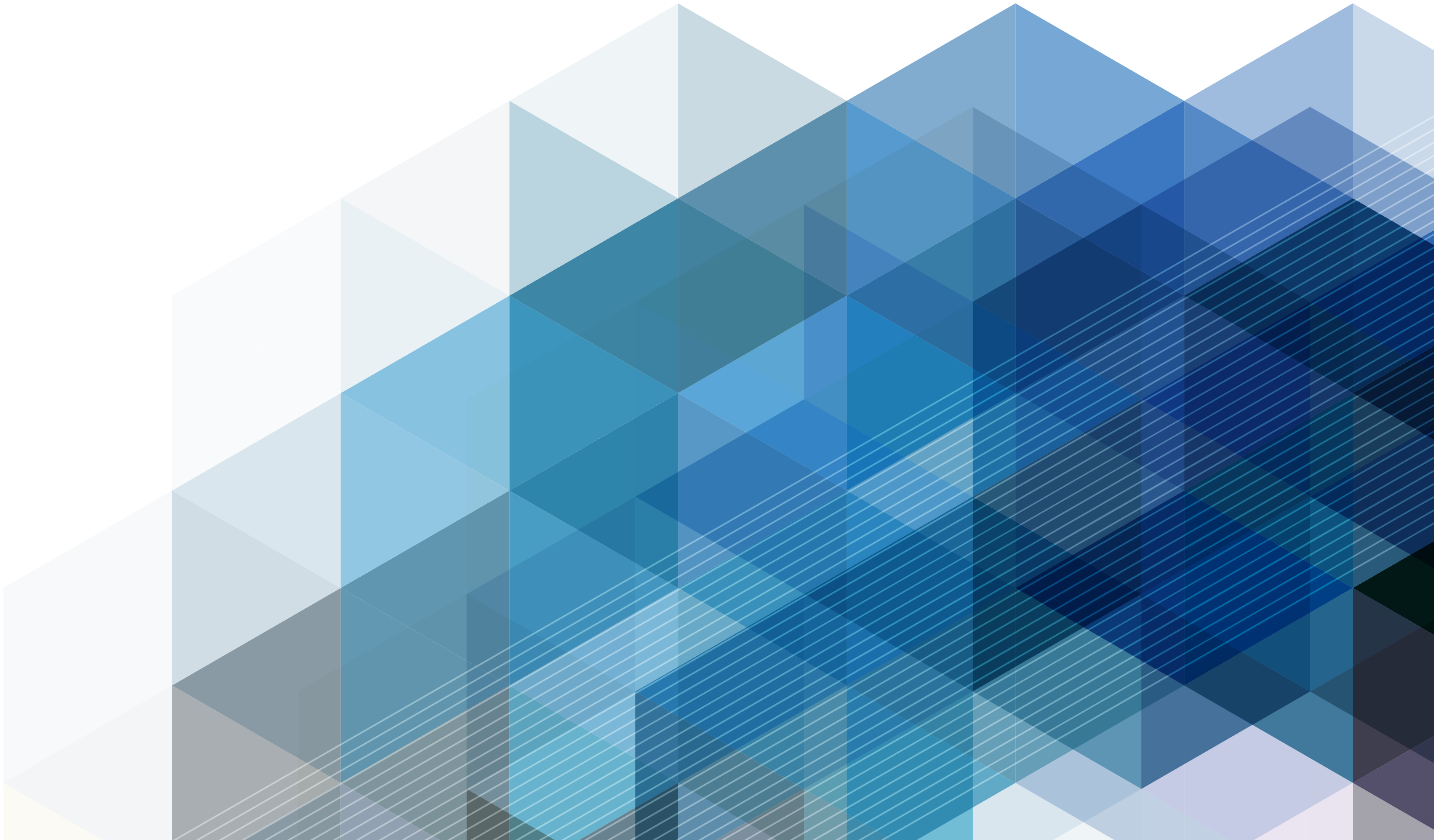
MarkMonitor
Protecting brands in the digital world

Clarivate
Analytics

Domain Management Handbook

A reference guide of industry leading best practices for managing corporate domain portfolios



CONTENTS

INTRODUCTION

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 domains are often managed in a manner similar to trademarks, the complexities associated with domains are far more intricate. Unlike trademarks, domain name restrictions and requirements change rapidly, making it difficult to stay current on all changes.

> *Domain strategies must evolve as the market continues to transform itself.*

Historically, registering broad variations and misspellings was a viable approach for protecting brands online, the Domain Name System (DNS) was not a target for cyber criminals and politically motivated hacktivists, and it used to be that there were just a few dozen top-level domains (TLDs) of real importance.

More than ever, it is essential for companies to balance the need for promotion with protection by making intelligent registration decisions. They also should ensure that domain assets, once registered, are completely secure. And on top of it all, companies need to make sure that they are effectively managing the entire domain name lifecycle, which includes directing domains to appropriate content, letting unnecessary names expire, and potentially selling unused and valuable names to fund new registrations and policing efforts.

So where to begin?

Based on our 15-plus years of experience as the industry's first corporate-only domain registrar, we've developed the best practices contained within this handbook to provide domain administrators with a reference guide for managing an ever-changing environment.

Undoubtedly our guidance has changed significantly over the years as the landscape also has changed. And, you can rest assured that our guidance will continue to evolve as the market continues to transform itself.

CHAPTER ONE

DOMAIN REGISTRATION BASICS

Registration Best Practices

IDENTIFY CORE, KEY, IMPORTANT AND LIMITED BRANDS

Separating brands into categories will help ensure appropriate levels of domain registration coverage. While this may seem like a simple task, levels can sometimes be difficult to distinguish. Looking at existing trademark holdings, as well as instances of abuse, is one way to objectively determine the level of importance a brand holds on the Internet.

As a general rule for global companies, brands with trademark registrations in more than 30 countries are typically considered to be core, and those registered in 15 to 30 countries are typically considered key.

Important brands may be those that are specific to a particular region of the world, and limited brands often consist of slogans, which are used to support specific campaigns for a limited period of time.

MATCH REGISTRATION COVERAGE WITH BRAND TYPE

Brands determined to be core or key typically require greater coverage. Variations, misspellings and typosquats should be considered within a .com domain for these assets.

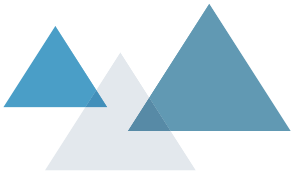
For important or limited brands, focus should be placed upon exact-match registrations, unless significant cybersquatting exists. Brands with high instances of registration abuse in a .com domain should be treated as a key brand.

ALIGN TRADEMARKS WITH DOMAINS

MarkMonitor® recommends that domain registrations align with trademark registrations, so if a French trademark exists, the corresponding .fr domain is also registered. Using an automated tool can help accomplish this quickly and accurately.

30

As a general rule, brands with trademark registrations in more than 30 countries are typically considered to be core, and those registered in 15 to 30 countries are typically considered key.



WHEN DETERMINING WHERE TO REGISTER, FOCUS ON CORPORATE ONLINE OBJECTIVES

When identifying where to register, a company should ensure that domains provide adequate coverage to meet corporate objectives. It is also important to think about future marketing needs. If the objective is to maximize exposure on the Web and generate e-commerce revenue worldwide, the following should be considered:

- Geographic locations where you have offices or do business
- TLDs that support worldwide sales and marketing efforts
- All legacy generic top-level domains (gTLDs)
- Select new gTLDs
- Top 10, 25 or 50 e-commerce countries

UNDERSTAND YOUR COMPANY'S TOLERANCE FOR RISK

If your company's culture is one that is extremely risk adverse, registering defensively may make sense. Those extensions that are most at risk for cybersquatting include:

- Popular legacy gTLDs
- Free or low-cost, unrestricted country code top-level domains (ccTLD) extensions
- Unrestricted, generic new gTLDs

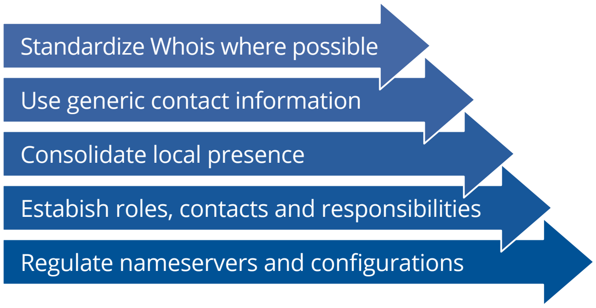
While registering defensively (especially misspellings) can help to ensure that your clients find you, it does not negate the need for actively monitoring for abuse.

UTILIZE STANDARD WHOIS CONTACTS

Standard Whois information should be used whenever possible to allow for uniformity throughout a domain portfolio. Only legitimate information should appear on Whois records. The registrant contact should be the same as the business registration or trademark owner. The domain contact listed on the Whois for the registrant, administrator, technical and billing contacts should be generic whenever possible, such as "Domain Administrator" or "DNS Administrator." When an actual person's name is needed on Whois information, that person should be the administrative contact whenever possible.

The email address for all contacts should also be generic, such as domains@companyname.com, and have the ability to send and receive email. The same applies to phone and fax numbers; it's best to use the company's main contact numbers.

When local presence information is needed to secure a domain, the same local presence information should be used whenever possible. If registering a domain name requires the administrative contact actually live in the country that matches the domain extension, the person chosen should be a director of the company or an employee who has full signing authority for any changes needed to the domain.



Standardize Whois where possible

Use generic contact information

Consolidate local presence

Estabish roles, contacts and responsibilities

Regulate nameservers and configurations

EMPLOY DEFAULT NAMESERVERS

In addition to standardizing Whois contacts, standard nameservers also should be employed. Using a standard set of nameservers eliminates the need for maintaining multiple DNS hosting vendors, sites, logins, etc.

Did You Know?

Upwards of **40%-60%** of corporate domain name portfolios are not pointing to live content today. Utilizing your registrar's Web forwarding capability is a quick and easy way to ensure that valuable Web traffic is not lost or redirected.

POINT EVERY DOMAIN TO LIVE CONTENT

Every domain in a portfolio should point to a live site or a parked page. Domains that are not pointing to live content may be redirected by Internet service providers (ISPs) or browsers to other content. Be aware that masked domains should forward to an "under construction" or otherwise generic Web page. Misspellings and defensive registrations should be pointed to appropriate content so that visitors find the content for which they are looking and ccTLDs should point to localized, native content.

UNDERSTAND THE VALUE OF YOUR DOMAIN PORTFOLIO

Whether you are using a registrar's DNS, your own, or a trusted third-party provider, tracking DNS queries and Web forwarding statistics provides valuable traffic data enabling you to understand the value of defensive holdings.

PROTECT VALUABLE DOMAINS

If a domain will be used for transactional purposes, advanced locking mechanisms, such as Registry Locking, should be implemented. The advanced locking helps protect against unintentional domain modifications, unauthorized domain transfers and malicious attacks. Highly valued domains should also be registered for the maximum allowable term and be set to automatically renew each year. (For a comprehensive list of domain security best practices, see Chapter 2.)

MONITOR FOR ABUSE

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.

Domain monitoring can be accomplished by searching through zone files for newly added domains 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 or 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, sending a Cease and Desist (C&D) letter, filing a Uniform Domain Name Dispute Resolution Policy (UDRP) or Uniform Rapid Suspension (URS), or challenging the accuracy of the Whois record, if the name falls into the hands of a suspicious individual or entity.

Transfer Best Practices

USE THIS OPPORTUNITY TO PARE BACK PORTFOLIOS

Deciding to transfer a corporate domain portfolio from one registrar to another is a big decision with a significant requirement of resources. When taking this step and reviewing every domain under management, it also makes sense to use this opportunity to determine which domains are no longer needed.

Here are some situations in which it may be appropriate to not transfer domains, allowing them to expire at their current registrar:

- Brands or products that have been discontinued
- Promotions or sweepstakes that have expired
- Companies that have been dissolved and are no longer in existence
- Outdated marketing campaigns that are no longer in use
- Registrations of variations, or in TLDs that now have limited value

Before deciding to let names expire at their current registrar, check with the appropriate stakeholders within your company to get sign-off on the request. Be sure to review traffic to these sites by checking DNS queries or Web forward statistics to ensure that active sites are not allowed to expire.

RENEW SOON-TO-EXPIRE DOMAINS

In order to protect against unintended expiration, gTLDs that are set to expire within 21 days should be renewed at their current registrar; ccTLDs that are set to expire within 45 days should be renewed at their current registrar.

EXPECT A COMPREHENSIVE TRANSFER PLAN

When transferring a corporate portfolio, a comprehensive transfer plan that takes into account each domain name and its level of importance, current expiration date, TLD type and action required to transfer should be provided by your registrar. Generally, portfolio transfers should occur in four phases:

- **Phase 1 - gTLDs and automated ccTLDs**

  Typically, the majority of domains within a corporate portfolio are gTLDs and automated ccTLDs. These domains can often be transferred within the first month, provided there is cooperation from outgoing registrars and authorization codes are received in a timely manner. Special care should be given to high profile and mission-critical domains.

- **Phase 2 - ccTLDs Requiring Login, Password or Authorization Codes**

  These domains can be transferred by providing the login, password or authorization codes associated to the domains. Transfer of these domains can be relatively straightforward, and it may be possible to complete the transfer of these domains within the first month.

- **Phase 3 - ccTLDs Requiring a Letter of Authority (LOA) or Email Approval**

  Some of these domains can be processed via completion of an LOA by the domain owner or via email approval by the current contacts for the domains. In most cases, a standard LOA on the company's letterhead will suffice, but exceptions to this include situations where the company is not the registered owner, where there is a local language requirement for the LOA, and where the LOA must be notarized or the original provided.

- **Phase 4 - ccTLDs Requiring Paperwork**

  These domains are the most complicated to process, as paperwork and documentary evidence are required. These transfers typically are completed within three to eight weeks depending upon the registry processing times, which are beyond the registrar's control.

PROVIDE NECESSARY DOCUMENTATION UPFRONT

Before the transfer process begins, be prepared to provide the following to your registrar:

- Logins, passwords and authorization codes from the outgoing registrar
- LOA for each registrant (owner) of the domains
- Email approval either from the current registrar or Whois contacts
- Paperwork specific to the registry requiring completion by current Whois contacts

TAKE SPECIAL CARE WITH NAMESERVERS

Prior to undertaking any domain name transfer, you should inventory every nameserver associated with every domain within the portfolio. If your company is managing DNS internally or using a third-party DNS provider, such as Neustar, then no special action is required.

However, any domains using the outgoing registrar's nameservers and DNS should be flagged, and DNS should be configured on the gaining registrar's nameservers.

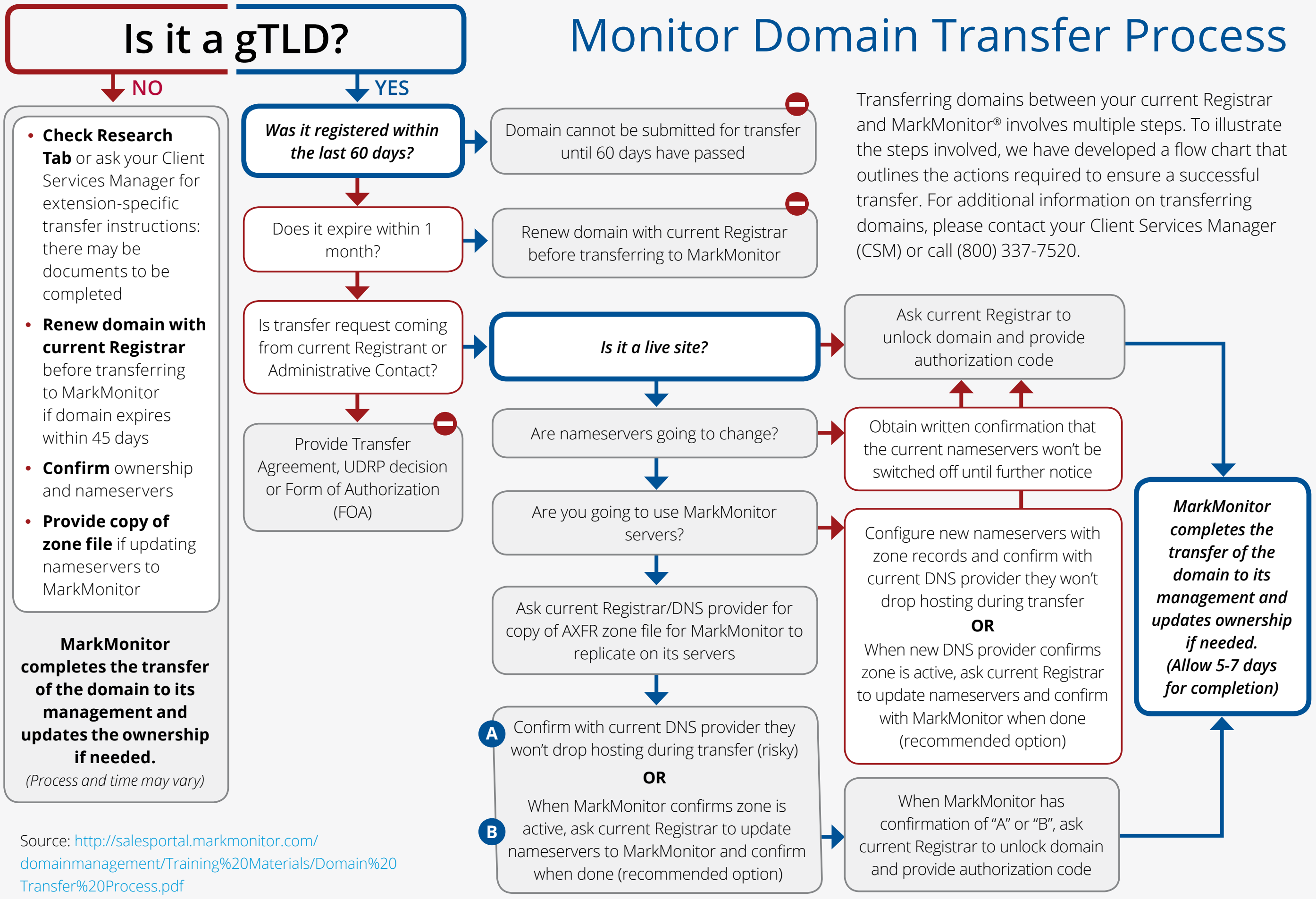
NEVER initiate a domain name transfer without ensuring that newly applied nameservers are correctly configured.

REQUEST WEEKLY REPORTING

Expect a weekly, summarized status report of progress and remaining actions required to complete the transfer plan. Having access to this information will help to alleviate concerns, set expectations and uncover any potential issues so that they can be resolved as quickly as possible.

Monitor Domain Transfer Process

Transferring domains between your current Registrar and MarkMonitor® involves multiple steps. To illustrate the steps involved, we have developed a flow chart that outlines the actions required to ensure a successful transfer. For additional information on transferring domains, please contact your Client Services Manager (CSM) or call (800) 337-7520.



Is it a gTLD?

NO

- **Check Research Tab** or ask your Client Services Manager for extension-specific transfer instructions: there may be documents to be completed
- **Renew domain with current Registrar** before transferring to MarkMonitor if domain expires within 45 days
- **Confirm** ownership and nameservers
- **Provide copy of zone file** if updating nameservers to MarkMonitor

MarkMonitor completes the transfer of the domain to its management and updates the ownership if needed.

(Process and time may vary)

YES

Was it registered within the last 60 days? → Domain cannot be submitted for transfer until 60 days have passed

Does it expire within 1 month? → Renew domain with current Registrar before transferring to MarkMonitor

Is transfer request coming from current Registrant or Administrative Contact? → ***Is it a live site?*** → Ask current Registrar to unlock domain and provide authorization code

Provide Transfer Agreement, UDRP decision or Form of Authorization (FOA)

Are nameservers going to change? → Obtain written confirmation that the current nameservers won't be switched off until further notice

Are you going to use MarkMonitor servers? → Configure new nameservers with zone records and confirm with current DNS provider they won't drop hosting during transfer **OR** When new DNS provider confirms zone is active, ask current Registrar to update nameservers and confirm with MarkMonitor when done (recommended option)

Ask current Registrar/DNS provider for copy of AXFR zone file for MarkMonitor to replicate on its servers

A Confirm with current DNS provider they won't drop hosting during transfer (risky)

OR

B When MarkMonitor confirms zone is active, ask current Registrar to update nameservers to MarkMonitor and confirm when done (recommended option)

→ When MarkMonitor has confirmation of "A" or "B", ask current Registrar to unlock domain and provide authorization code

MarkMonitor completes the transfer of the domain to its management and updates ownership if needed. (Allow 5-7 days for completion)

Source: http://salesportal.markmonitor.com/domainmanagement/Training%20Materials/Domain%20Transfer%20Process.pdf

CHAPTER TWO

NEW gTLDs

New gTLD Best Practices

IDENTIFY AND SUBMIT TRADEMARKS TO THE TRADEMARK CLEARINGHOUSE

The Trademark Clearinghouse (TMCH) serves as a central repository of authenticated trademark information. The information contained within the TMCH will be used to enable Sunrise Registrations and Domain Name Blocking.

There is no one-size-fits-all when it comes to developing a registration and blocking strategy.

REVIEW ALL NEW GTLDS AND REGISTER SELECTIVELY

With approximately 1,000 new gTLDs now delegated, many companies have fallen into a registration rhythm, and the approaches are ranging from very minimal registration and blocking strategies for one or two core brands, to registrations of multiple brands in every single new gTLD registry. Decisions of what to register are based on a risk tolerance continuum and focus on relevance of the TLD, and risk of a monitoring only approach.

Most companies are looking to register exact matches of their core trademarks in registries where there is a close correlation between the brand and the TLD. For example, financial institutions generally should register TLDs such as .bank, .loan(s), and .mortgage, provided they meet eligibility requirements. Identifying these kinds of close matches is easy, especially given the number of open and restricted new gTLDs is just under 620.[1]

The more difficult question is where to register in non-Latin TLDs. When it comes to non-Latin registrations, companies should make best efforts to understand how brands are marketed internationally. If they are marketed using non-Latin characters, then consider registering in the Internationalized Domain Name (IDN) TLDs, assuming that there is a nexus between the brand and the TLD. However, mixing character scripts and registering Latin second-levels with non-Latin top-levels is generally discouraged.

[1] ICANN, New Generic Top Level Domains, http://newgtlds.icann.org/en/program-status/statistics, March 2016.

Companies also have to make difficult decisions about whether it makes sense to register in any of the city or geographic TLDs. In this situation, companies need to think about whether they are actively marketing or promoting their brands in these cities or regions.

In addition, there are certain categories of registries which pose their own special risks, including gripe (.wtf and .sucks), vice (.sex and .poker), corporate identifier (.inc and .gmbh) and charitable (.foundation and .charity) TLDs — and companies must determine their tolerance for risk when planning their registration and blocking strategies around these.

And finally, there are all of the truly generic new gTLD registries, including . web, .blog and .news — and again, there are difficult decisions to be made, as there is no one-size-fits-all when it comes to developing a registration and blocking strategy.

TAKE ADVANTAGE OF BLOCKING – BUT BEWARE

Donuts Inc., which applied for over 300 new gTLDs and Rightside Registry, which applied for over 30 new gTLDs, are both offering submissions to their respective Domain Protected Marks Lists (DPMLs).[2] This service essentially enables brand owners to block a string containing a trademark that has been validated against the TMCH across every TLD managed by either Donuts or Rightside Registry. It is important to note that exact matches can be protected as well as ANY string containing a validated trademark.

This means that if MarkMonitor had successfully submitted a trademark for "MarkMonitor" to the TMCH, strings such as MarkMonitorProducts, MarkMonitorServices or MarkMonitorClients could be blocked across all of the Donuts TLDs and/or Rightside Registry TLDs.

The downside is there will be fees associated with each protected string. Also, any blocked registration can be overridden and registered as a domain by anyone who owns a validated TMCH submission.

Moreover, any names that are identified as premium are ineligible for blocking. This means that if a trademark is dictionary term, is a first name or surname, or is a three-letter acronym — there is a distinct possibility it will be deemed as premium by the registry and therefore ineligible for blocking. To complicate matters, premium name lists are only distributed just prior to the launch of every Sunrise Period for Donuts and Rightside Registry TLDs.

These are two examples of large TLD operators that have blocking options. Other operators have blocking options as well with their own unique pricing structure and level of protection. All that said, for companies with a unique trademark and where risk and relevance is high in the applicable TLDs, blocking can be a cost-effective approach. However, for others the cost benefit or level of protection may not justify a blocking approach.

[2] ICANN, "New Generic Top Level Domains," ICANN.org, March 2016.

ENSURE THAT YOUR EXISTING REGISTRAR IS COMMITTED TO PROVIDING NEW gTLDs

Select a registrar that is committed to providing registration services for all new gTLDs. Working with a single registrar (as opposed to multiple registrars) will help to ease complexity.

BECOME FAMILIAR WITH NEW RIGHTS PROTECTION MECHANISMS

The Internet Corporation for Assigned Names and Numbers (ICANN) has adopted a number of new rights protection mechanisms as part of the new gTLD program, including Trademark Claims, Sunrise Registrations, the Uniform Rapid Suspension (URS), the Post-Delegation Dispute Resolution Procedure (PDDRP) and the Registry Restriction Dispute Resolution Procedure (RRDRP).

Trademark Claims

During the first 90 days of general registration, if a domain submitted for registration is an identical match to an authenticated trademark in the TMCH, the Trademark Claims service will provide notification to the prospective registrant during the registrar workflow that the mark is included in the TMCH.

Sunrise Registrations

Sunrise Registration periods give trademark holders in the TMCH priority to register domains before they are available to the general public, assuming all eligibility requirements are met.

Uniform Rapid Suspension (URS)

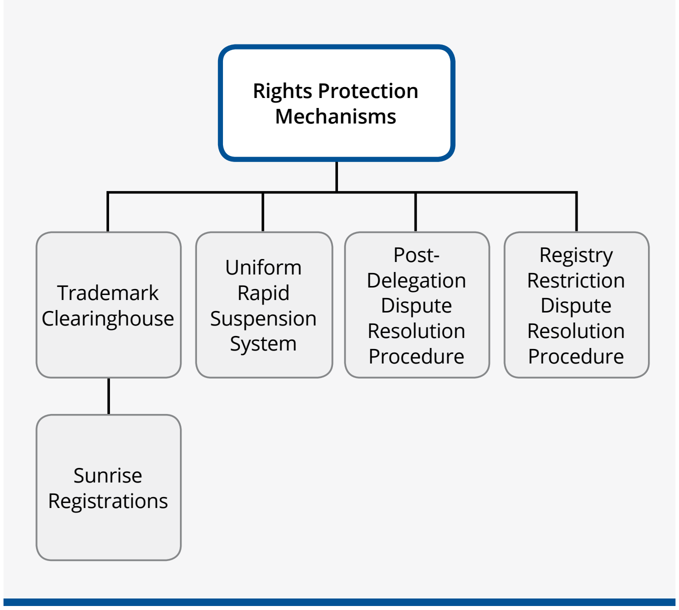
The URS was designed to provide a cost-effective, expedited process to address issues of trademark infringement and abuse. Domains are suspended for the remainder of the registration term but will be available again for registration once the domain expires.

Post-Delegation Dispute Resolution Procedure (PDDRP)

The PDDRP will also provide rights holders with the ability to file complaints against registries that 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).

Registry Restriction Dispute Resolution Procedure (RRDRP)

The RRDRP is a complaint procedure for community-based gTLDs. The complainant must prove that the TLD operator violated the terms of the community-based restrictions in its agreement and that there is measurable harm to the complainant and the community named by the objector.

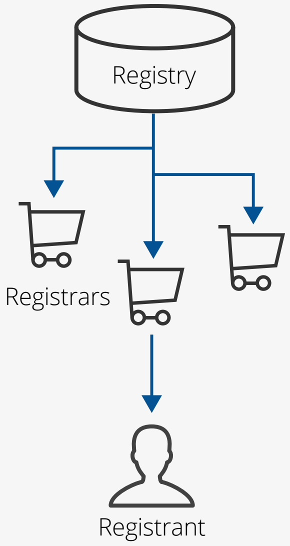

Rights Protection Mechanisms
Trademark Clearinghouse
Uniform Rapid Suspension System
Post-Delegation Dispute Resolution Procedure
Registry Restriction Dispute Resolution Procedure
Sunrise Registrations

CHAPTER THREE

DOMAIN SECURITY

Understanding the Vulnerabilities

The Domain Ecosystem



There are three primary entity types in the domain name ecosystem: registries, registrars and registrants.

Registries provide direct services to registrars and in most instances are the authoritative source for domain ownership information (with exception of .com, .net and .jobs), lock status and nameserver settings. The registry can be thought of as the wholesaler in this ecosystem.

Registrars provide direct services to domain name registrants, and can be thought of as the retailer. Registrars process domain name registrations and pass all necessary information through to the registry for entry into their centralized registry database.

The **registrant** is the owner of a domain name and responsible for maintaining contact information, locking status, nameserver settings and renewals via their registrar.

There are potential vulnerabilities within each function of the ecosystem. These include various types of breaches, as well as hackers and hacktivists that have been actively targeting the domain industry for years.

In addition, it is important to note that registries, registrars and registrants are not impervious to inadvertent mistakes — which can result in domain name downtime, or in the most severe case, loss of a domain.

REGISTRAR OUTAGES AND HACKS

Over the past several years, a number of high-profile registrars have been breached through social engineering or more technical exploits. These often result in domains being forwarded to politically motivated sites, and in some cases worse.

In a number of other cases, registrars have inadvertently updated nameservers, resulting in website downtime for registrants.

REGISTRY BREACHES

Popular ccTLD registries such as .cn (China), .be (Belgium) and .my (Malaysia) have all been impacted by issues arising from Distributed Denial of Service (DDoS) to Social Engineering and Brute Force attacks. With more than 30 registry security breaches within the last three years, the number of incidents has reached an all-time high, although there are indications that the frequency of new incidents is beginning to decrease.

PHISHING AND OTHER SOCIAL ENGINEERING ATTACKS

Domain name registrants also need to evaluate the weakness of their human links. Some companies have been victimized by simple social engineering tricks, such as a hacker looking up the registrar for a site, calling the registrar, claiming to be a new technical contact and asking for the passwords so they can proceed with their work. In many cases, a user ID and password combination is all an attacker needs to gain control of an entire domain name portfolio.

COLLECTION OF CREDENTIAL INFORMATION BY MALWARE

Another type of attack involves the targeted deployment of malware, such as keyloggers. In this type of attack, domain administrators are tricked into clicking on a website link or opening an attachment in an email. These keyloggers track logins and passwords for corporate domain name management portals. With this credential information, scammers can unlock and hijack domains, update nameservers and even change DNS settings — any of which could result in site downtime or the proliferation of more malware to unsuspecting website visitors.

CACHE POISONING OR PHARMING

Recursive or caching servers are another point of vulnerability if they are breached. They can be used in man-in-the-middle attacks, in which hackers update a cached Internet Protocol (IP) address to a malicious website and capture user IDs and passwords while forwarding traffic to and from the real site, leaving the victims unaware of the malfeasance.

Domain Security Best Practices

CONSOLIDATE YOUR PORTFOLIO OF DOMAINS

In the past, it was not uncommon for IT, marketing, and legal to all be involved in the registration of domains. Consolidating your portfolio allows you to discover all of the registrations you have. This not only enables you to make smart decisions about what to register, but helps to ensure that the names you have registered are not at risk if somebody leaves the company.

Know which domains you own and make sure you have a global, centralized view of all your domains across all offices and locations. Maintaining careful records and keeping track of your entire domain portfolio is half the battle. Partnering with a corporate-only registrar committed to supporting new gTLDs and ccTLDs globally is key.

Quick Tip

1. Compare trademark holdings against domain name registrations
2. Utilize Reverse Whois to uncover lost registrations
3. Work with marketing, IT, e-commerce, and legal to identify all existing registrations

The first step in implementing this best practice is to compare your domains to your portfolio of trademarks. Use Reverse Whois to determine all the domains that have been registered by specific employees. Ask around within your organization to see who might have been involved in registration in the past. The goal is a complete inventory, so expect to invest a few weeks or even months to get it done right.

Once you have completed your inventory, we recommend transferring all domains to a single registrar. You will then be able to ensure you have the right security settings.

ENSURE YOUR REGISTRAR HAS SOLID AND EXTENSIVE INDUSTRY RELATIONSHIPS

Expect that there may be security issues with many new registries out there. Well-known events such as the 2014 outbreak of the Heartbleed virus point to the critical need for a registrar that has extensive industry relationships.

You need to work with a registrar that can quickly contact the registry to resolve problems. Many registries will not engage directly with registrants. If, for example, the registry has been breached, your registrar will need to know whom to contact.

Make sure your registrar is well established and experienced. Your registrar should function as part of the security ecosystem, with strong relationships with other registrars, top ISPs, security organizations, browser partners, major software developers and standards groups that will keep it well informed as new threats emerge. Speed matters — these relationships will enable your registrar to quickly rectify any security breaches that do occur. Seek out a registrar that offers both guidance and deep experience in security, as well as domain management.

MONITOR CRITICAL DOMAINS

It is necessary your registrar monitor for differences between the nameservers stored at the registry compared to the nameservers stored in their databases. A mismatch could be the first sign someone has broken into a registry system and made an unauthorized update.

Your registrar should regularly monitor changes to nameservers, even on an hourly basis, for your core domains.

Did You Know?

Sophisticated corporate registrars will often notify you of registry breaches before your own internal security teams do.

RECEIVE AUTOMATED NOTIFICATIONS OF EVERY DOMAIN NAME UPDATE

Should someone gain access to an account, if it is breached in any way — whether by a disgruntled employee, hacker or by mistake — you need to know the domain is being updated.

Secure account management allows automatic notifications to a specified, secure email address when any change to a domain occurs. Once enabled, this service will automatically send a system-generated email to the secure email address, notifying the recipient of any change that was made.

SET REGISTRATION POLICIES

Companies must employ internal domain name policy guidelines. The lack of a policy means things might get out of hand. The policy document should include:

- Who is allowed to request a registration
- Who is allowed to approve a registration
- What the process is to register a domain
- Budget limitations
- Approvals needed
- Where the names point to

IMPLEMENT LOCKING AT APPROPRIATE LEVELS

Set Every Domain to Locked

In response to the threat of domain name hijacking, ensure all domains under management are locked, making them unavailable for transfer. All domains should be created, configured and then locked.

Implement Registrar Locking

There is also an elevated locking mechanism, sometimes referred to as a registrar lock or a super lock, that essentially freezes all domain configurations until the registrar unlocks them upon completion of a customer-specified security protocol.

Companies control the level of complexity associated with their specific protocol, and domains are made available for updating through the portal only when these security protocols are accurately completed. This extra level of security should be applied to your most mission-critical domains such as transactional sites, email systems, intranets and site-supporting applications.

Demand Registry Locking

Generic domain locking can still be exploited by an attacker who updates nameservers and redirects customers to illegitimate websites without transferring actual control of the domain from one registrar to another. To combat this, another step is registry locking or premium locking, which makes the domain unavailable for any updates. This method of locking is currently available for .com, .net, .org and more than two dozen ccTLDs.

Quick Tip

Locking domains at the registry is by far the most effective method for ensuring the security of mission-critical registrations.

PROTECT AUTHORIZATION CODES

Every gTLD and some ccTLDs have a unique authorization code. When a domain is transferred from one registrar to another, this authorization code must be supplied. You are at risk if these authorization codes are shown in your registrar's portal. We recommend your registrar keep these codes separate and only send them via secure email.

Authorization codes should be considered extremely confidential. Anyone who knows these codes can request the transfer of any domain in an unlocked state. The only time you should share an authorization code is if you are transferring the domain to another registrar.

EMPLOY 2FA FOR ACCESSING A DOMAIN MANAGEMENT PORTAL OR A DNS MANAGEMENT PORTAL

Two-Factor Authentication, also known as 2FA, is an extra layer of security that requires not only a password and username, but also something that only the user can provide, such as a one-time password via a physical token. Using a username and password together with a piece of information only the user knows makes it harder for potential intruders to gain access, even if login credentials are compromised.

You should require your registrar to utilize 2FA as well as your outsourced DNS provider if you use one.

Did You Know?

2FA protects against unauthorized access to domain management portals resulting from lost or stolen passwords by requiring an additional one-time password that only the legitimate user knows.

NEVER SHARE LOGIN CREDENTIALS FOR DOMAIN AND DNS MANAGEMENT PORTALS

If your registrar is not set up for enterprise-wide use it might only give you one login and password that needs to be shared by multiple users within your organization. This is a security risk. A registrar that allows each user in your organization to have a unique login or password will be more secure. Never share your login credentials and never reveal your password to another person.

LIMIT AND SPECIFY USER RIGHTS FOR MANAGEMENT OF DOMAINS

You should ensure the user rights (full access, read-only or no access) you have deployed match the importance of the domain. Consider limiting the ability to update nameservers, locking status and ownership information based upon the needs of each user. You don't need to give full access to everyone. Evaluate your critical domains and determine, of all your users, who actually needs access.

CONTINUALLY MANAGE AND REVIEW USER ACCOUNTS

Expect that people will change jobs within the organization or leave the company. As they rotate out of domain administrator responsibility, make sure you delete inactive users. Consider making the deletion of users leaving the company a standard part of exit interviews. A frequent review of secondary account users is necessary to remove any users who may no longer be with the company or who may have changed job roles. It is also important to regularly review user permissions to ensure that proper permissions are applied to each user. Managing user accounts is critical to maintaining a clear list of current and authorized users of your accounts.

REQUIRE MANDATORY PASSWORD UPDATES

Password management options can force password changes every 30, 60 or 90 days. Implement forced password changes to make it more difficult for scammers to gain access to valuable login credentials. This is basic security for any networked computer system.

IMPLEMENT IP ACCESS RESTRICTIONS

Restricting IP access can limit logins from networks outside of the company. Prevent unauthorized logins and protect against lost, stolen or compromised login credentials with IP access restrictions. You can choose a specific IP address or a range which limits entry points to your system.

UTILIZE A CORPORATE-ONLY, HARDENED REGISTRAR

Ensure that your registrar employs a “hardened” portal — one that employs constant checks for security and code vulnerabilities. They should employ third-party verified testers that conduct penetration testing. Your registrar should monitor for suspicious login attempts and report from part of the world they originate. Unlike a retail registrar, corporate registrars should have defined policies with regard to which people they interact with at your organization so that they are impervious to social engineering attacks.

Quick Tip

A corporate registrar must have a proven track record of being able to stay on top of new exploits, researching and understanding new vulnerabilities AND must be able to demonstrate use of strong internal security controls and best practices.

IMPLEMENT DOMAIN NAME SYSTEM SECURITY EXTENSIONS (DNSSEC)

DNSSEC prevents cache poisoning. It is used to ensure that caching server records are accurate and complete. It provides a way to be sure that you are communicating with the correct website or other service. DNSSEC provides a level of additional security where the web browser can check to make sure the DNS information is correct and was not modified.

Signing your domain with DNSSEC involves two components:

1. The *registrar* of your domain name needs to be able to accept what are called Delegation Signor (DS) records and be able to send those to the TLD Registry for your domain (e.g., .com, .org, .net).
2. The DNS *hosting provider* that operates the DNS nameservers for your domain must support DNSSEC and be able to sign (and re-sign) your DNS zone files.

Sometimes both of these components are one service offered by a registrar. Other times, the DNS records for your domain might be hosted at another provider — or you might host on your own DNS servers.

There are two scenarios for signing DNSSEC:

1. Domain name owner maintains their own nameservers
   - Create keys and enter them in the zone
   - Generate signed zone
   - Upload DS records to registry via registrar
   - Publish zone
2. Domain name owner relies on a third-party DNS provider
   - Contact the provider for instructions to turn on DNSSEC
   - Upload DS records to registry via registrar

CHAPTER FOUR

DOMAIN RECOVERY

Understanding the Need

Domain recovery is the umbrella under which all methods of recovering or securing domains of business significance fall. In cases where the domain(s) in question align with pre-existing brands (and therefore pre-existing rights), a broader range of options exists. In the case of already-registered domains, which are required for a new branding initiative or campaign (and lack pre-existing legal rights), anonymous acquisition tends to be the only viable short-term option.

> *Brand owners should develop a system of prioritizing and ranking infringements to allow for a recovery strategy that matches the significance of the threat and associated business impact.*

The following recovery options exist:

- Cease and Desist (C&D) letter
- Uniform Dispute Resolution Policy (UDRP)
- Uniform Rapid Suspension (URS)
- Alternate Dispute Resolution (ADR)
- Anticybersquatting Consumer Protection Act (ACPA) lawsuit
- Domain backorders
- Anonymous acquisition

Domain Recovery Best Practices

Many companies are targeted on a scale that makes recovery of all infringing domains financially impractical. Brand owners should develop a system of prioritizing and ranking infringements to allow for a recovery strategy that matches the significance of the threat and associated business impact. A domain pointed to a pay-per-click page should not be regarded with the same urgency as a domain being used as a copycat phishing site or as domain serving malware. Considering all available recovery options in conjunction with an internal assessment of relative urgency, cost considerations, business significance and threat level allows for effective decision making on a case-by-case basis. The toolbox analogy is apt: each recovery option serves a purpose, but each option is not equally effective in dealing with a specific situation.

DOMAIN RECOVERY OPTIONS

Cease and Desist Letter (C&D)

A C&D letter is a demand to turn over a domain or bring down content based upon pre-existing legal rights. If a domain name does not infringe on a trademark, a C&D is limited to a demand to remove content. Such a C&D is an enforcement option rather than a recovery option. C&Ds are non-binding and are frequently ignored by experienced cybersquatters. C&Ds have a much higher success rate with registrants who may have registered an infringing domain without knowledge of their infringement. If acquiring a domain is mission critical and the dispute resolution option (UDRP or ADR) is judged relatively weak, consider the implications of sending a C&D. Subsequent attempts to purchase the domain may result in non-responsiveness or price-gouging by the registrant.

C&Ds are a good option if:

- Quick recovery is not a critical consideration
- The domain is regarded as “nice to have” rather than mission critical
- The UDRP or ADR option is a viable escalation, should the C&D fail

The Uniform Dispute Resolution Policy (UDRP)

The UDRP applies to all gTLDs (traditional gTLDs such as .com, as well as new gTLDs such as .email). The UDRP has also been adopted by some ccTLD registries as the governing dispute resolution policy. Most ccTLDs that have not adopted the UDRP adhere to an Alternative Dispute Resolution (ADR) policy, which is TLD specific. A small number of ccTLD registries do not offer a dispute resolution option and the only recovery option in these jurisdictions is a lawsuit, filed within that jurisdiction. A victorious complainant may choose to have subject domain(s) canceled (rarely requested) or transferred to complainant control. Three to four months is the typical timeframe for a UDRP decision.

The complainant in a successful UDRP must prove:

- The domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights;
- The registrant has no rights or legitimate interests in respect of the domain name; and
- The domain name has been registered and is being used in bad faith.

It is recommended UDRPs be filed by Intellectual Property (IP) attorneys, ideally an attorney with UDRP experience. While filing procedures are relatively straightforward, many UDRPs have been lost due to a counsel’s unfamiliarity with UDRP case law and precedent.

UDRP is a good option if:

- Quick recovery (< 3 months) is not a critical consideration
- Legal rights in the form of a registered or common law trademark exist
- Current usage violates the mark holder’s rights and/or represents a reputational or security issue

- Recovery is considered important enough to justify UDRP cost

Uniform Rapid Suspension

The URS is intended as an expedited and cost-effective alternative to the UDRP. Because the outcome of a successful URS is suspension of the DNS on a domain rather than transfer of the domain itself, the URS is not, technically speaking, a recovery option. The URS is applicable to all new gTLDs as well as .pw (Palau) and .us (United States). Decisions are usually received within 30 days of filing a complaint. Criteria are identical to the UDRP (see UDRP Section), but the URS has been positioned as a mechanism for *clear-cut* cases of abuse; the complainant's burden of proof is ostensibly greater in a URS filing than in a UDRP. The greatest drawback to the URS is that domains are only suspended for the remainder of their term or for an additional year at current market registration rates. *There is no option to transfer the domain into complainant control if victorious*. After suspension ends, domains become available again for registration.

URS is a good option if:

- Suspension rather than recovery is an acceptable outcome
- Strong legal rights in the form of a registered or common law trademark exist
- Current usage violates the mark holder's rights
- Reduced cost relative to a UDRP is appealing

Alternate Dispute Resolution (ADR)

ADR policies represent the TLD-specific dispute resolution policies enacted by most individual ccTLD registries. While criteria are frequently similar to the UDRP, significant differences in both procedural requirements (e.g., filing language) and policy elements (e.g., "registered and used in bad faith" versus "registered or used in bad faith") exist. ADR filings frequently require local IP counsel familiar with the TLD-specific policy.

ADR is a good option if:

- Quick recovery (< 3 months) is not a critical consideration
- Legal rights as defined by the TLD-specific policy exist
- Current usage violates the mark holder's rights and/or represents a reputational or security issue
- Recovery is considered important enough to justify ADR cost

Anticybersquatting Consumer Protection Act Lawsuit (ACPA)

Utilizing the ACPA is the lengthiest and costliest recovery option and is only considered in the most egregious cases of mass infringement. Unlike other domain recovery options, filing an ACPA case may allow for recovery of damages of up to $100,000 per infringing domain[3], in addition to recovery of the domain. While in rem filings against domains rather than registrants sometimes allow for suits against "ghostly" registrants who cannot be identified or located, they also eliminate the ability to collect monetary damages.

[3] U.S. Patent and Trademark Office, "U.S. Trademark Law: Federal Statutes," USPTO.gov, November 15, 2013.

Under the ACPA, a trademark owner may bring suit when a registrant:

- Has a bad faith intent to profit from the mark
- Registers, traffics in, or uses a domain name that is:
  - Identical or confusingly similar to a distinctive mark
  - Identical, confusingly similar to or dilutive of a famous mark

For a complete list of ccTLD-specific dispute resolution policies, see http://www.wipo.int/amc/en/domains/cctld_db/.

As with UDRPs, ACPA lawsuits should be handled by qualified IP counsel with pertinent experience. On balance, the ACPA is rarely the best recovery option, but exists to address extreme cases of domain-level infringement.

An ACPA lawsuit is a good option if:

- Recovery timeline is not the critical consideration
- Legal rights as defined by the ACPA exist
- The infringement is extreme in terms of scope and volume of domains and/or usage has a significant financial impact on the business
- Recovery and possibility of being awarded damages are considered important enough to justify time investment and cost of a lawsuit

Domain Backorders

Domain backordering or "domain snapping" is a passive recovery option that only allows for recovery of domains not renewed by their current owner. Backorder services send automated re-registration requests to the registry at the moment they are deleting. These services are well known and heavily used by domain speculators; manual monitoring and re-registration of domains should not be regarded as a viable option. Backorder services are not always successful and should not be relied upon for mission-critical domains. At times, if there are multiple interested parties, backorder services can result in backorder auctions, increasing cost.

Backorders are a good option if:

- A passive recovery option with no set timeline is acceptable
- The domain(s) is considered a "nice to have" rather than critical to the business
- Minimizing cost is desirable

Anonymous Acquisition

If an imminent launch or a lack of pre-existing rights precludes options such as the UDRP, anonymous acquisition may be the only viable option to secure a desired domain name. There also may be cases where purchase is simply quicker and more cost-effective than dispute resolution. While these factors may contribute to a decision to purchase a domain, it is recommended purchase is pursued only if UDRP or ADR is not a viable option. Rewarding cybersquatters emboldens the behavior and will exacerbate the problem for any company with a pattern of purchase in lieu of enforcement. Anonymous acquisition involves negotiation through a proxy entity to acquire a target domain. While unrealistic value expectations will always be part of the domain aftermarket landscape, anonymity often keeps purchase prices in a lower range than would be the case for a business openly negotiating purchase. Altruistic domain sellers are as common as unicorns. There are no guarantees of success, but an anonymous acquisition remains the most viable option to obtain a mission-critical domain if urgency or lack of rights do not allow for legal enforcement.

Anonymous acquisition is a good option if:

- Lack of rights or insufficient rights prevent use of UDRP, URS or ADR options
- Timeline does not allow for dispute resolution options (e.g., imminent launch)
- The country or region lacks a dispute resolution mechanism
- Cost to purchase is less than cost of dispute resolution

CHAPTER FIVE

NEW PRODUCT LAUNCH

Special Considerations

When companies launch a new product, service, title or campaign, the focus is often on trademark coverage. However, securing domains is just as important, if not more so, for many companies. In fact, domain registrations should be completed before any trademark application becomes public, to curb the potential for cybersquatting.

Prior to any launch, there are many important questions to be answered. For instance, are the domains available? Will the product be launched globally or domestically? Do you need to register in local languages to support global promotions? Is confidentiality a concern? It's critical to understand these requirements in order to properly support the product launch and minimize infringement.

New Product Launch Best Practices

CHECK GLOBAL AVAILABILITY

Check domain availability globally to identify which domains are still available and which are already registered to third parties. Also, be aware of existing domains that contain your new product name prior to launching any new product, service, title or campaign. Based on your findings, you may want to reconsider your naming approach. If domains are taken, you might also consider using a recovery service such as anonymous acquisition to obtain the domains.

ALWAYS USE A TRUSTED WHOIS LOOKUP

When checking global availability, lookups should be performed using a trusted Whois service. It is critical the Whois service used is secure, and any domains searched remain confidential. Using a Whois lookup that is not completely secure can result in the registration of the searched-for domains by a third party.

DETERMINE COVERAGE BASED UPON BRAND VALUE AND PROMOTIONAL STRATEGY

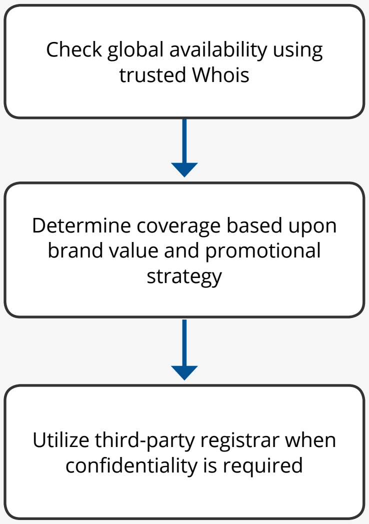
If you're launching a new brand domestically and there is a high tolerance for risk, your domain coverage will be on a smaller scale, focusing on legacy gTLDs and select new gTLDs. If the product is launching globally and your main objective is to maximize exposure on the Internet, the following should be considered:

- Native language translations to support geographic locations
- TLDs that support worldwide sales and marketing efforts
- All legacy gTLDs
- Select new gTLDs
- Top 10, 25 or 50 e-commerce countries

USE THIRD-PARTY REGISTRARS TO PROTECT CONFIDENTIALITY

Any registration that needs to remain confidential prior to public announcement should be completely masked using a third-party registrar. Domain speculators are notorious for monitoring registrations made via corporate registrars, as this information must be made publically available. Because of this, it is imperative third-party registrars are used for registration-sensitive domains, so any proprietary information is not detected and remains confidential.

New Product Launch Best Practices



Check global availability using trusted Whois

Determine coverage based upon brand value and promotional strategy

Utilize third-party registrar when confidentiality is required

CHAPTER SIX

PORTFOLIO RIGHTSIZING

Recognizing the Need

> *As a general concept, "portfolio rightsizing" entails regularly and critically reviewing a domain portfolio to identify registration gaps, out-of-policy registrations and legacy domains to keep a portfolio aligned with business goals.*

Over time, corporate domain portfolios have grown with a defense-first mindset. Intellectual property protection and domain retention have been the key factors shaping the scope of portfolios. The domain space has recently expanded to an unprecedented extent with the launch of hundreds of new extensions, making the traditional approach of retaining all legacy domains and securing brands across all pertinent extensions no longer viable. In this changing landscape, domain management strategies must also evolve. With the proper tools and strategic guidance, the explosion of new gTLDs does not necessitate increased domain budgets.

Portfolio Rightsizing Methodology

As a general concept, portfolio rightsizing entails regularly and critically reviewing a domain portfolio to identify registration gaps, out-of-policy registrations and legacy domains to keep a portfolio aligned with business goals. Once a portfolio is aligned with the business, portfolio value should be maximized by actively using most domains.

Portfolio Rightsizing Best Practices

In any domain portfolio, many domains will align with active brands. Many others will be less central to the business, although such domains may align with legacy products, services or campaigns. Other domains may sync with abandoned trademarks or may represent projects that were abandoned rather than launched.

The ability to review a domain portfolio in a segmented fashion provides domain managers with a powerful tool for making decisions regarding the health of the portfolio. Are core brands adequately protected? Are defunct brands and associated domains unnecessarily eating into budgets? Do hidden gems exist in the form of unused, unneeded domains that could be sold for significant return?

PUT YOUR DOMAINS TO WORK FOR YOU

Extensive coverage of core brands through associated domain registrations is common practice. Full gTLD coverage and coverage across many ccTLDs is typical. It is far too infrequent for the full complement of domains to be utilized effectively. A basic premise that applies to virtually all businesses is "traffic equals revenue." Site visits positively impact bottom line. For example, corebrand.info could be a significant source of traffic if redirected to corebrand.com. Likewise, brand-matching ccTLDs corebrand.ccTLD should point to a native language page or redirect to corebrand.com. Simply put, such domains should not be regarded as having strictly defensive value — put your domains to work for you!

IDENTIFY AND RETIRE LOW-VALUE, OFF-BRAND DOMAINS

Without regular maintenance, a corporate domain portfolio becomes more than a representation of the business. It becomes a museum, filled with ghosts of brands and campaigns past. Some deletion candidates are obvious (e.g., ourconference2011.com). Other domains may somewhat align with active brands, but represent poor registration choices (e.g., gary-indiana-loves-corebrand.biz). Taking a methodical, incremental approach to portfolio downsizing reduces risk. Set those triple-hyphen .mobi domains to do-not-renew and monitor status post-deletion to confirm that they are not being re-registered by speculators. Lapse .com domains judiciously; speculators concentrate almost exclusively on the .com space.

COMPARE ACTIVE TRADEMARKS AGAINST DOMAIN PORTFOLIOS TO UNCOVER BOTH GAPS AND BLOAT

Cross-referencing active and abandoned trademarks against domain registrations is an excellent method of gauging whether or not core brands are adequately protected in the domain space. This exercise also allows superfluous domains to be identified. If a trademark is registered in 10 jurisdictions and the corresponding TLDs have not been secured, it may reflect undefined or weakly defined registration policies. Alternately, if a mark was abandoned 10 years ago and the associated business, product or service is defunct, retention of the associated domains may simply represent a lack of portfolio maintenance.

CONSIDER SELLING UNUSED ASSETS

The new gTLD landscape merits consideration of revised domain portfolio management strategies in order to balance adequate online presence with cost. The substantial resale market can present opportunities to offset domain costs as domain portfolios continue to grow. Most domains were registered or otherwise acquired to protect a brand, to actively utilize, or both. Over time, active brands change, campaigns wind down and geographic presence may shift. Before exploring the sale of domains, it is critical to establish that a sale would not cause internal business disruption or otherwise compromise active brands. Unneeded domains may hold value from a few hundred to millions of dollars, and it's critical to understand the domain market in order to establish fair value for a domain. Use a domain sales service designed to carefully vet corporate domains for resale.

CHAPTER SEVEN

ACQUISITIONS AND DIVESTITURES

Lessons Learned

When a company goes through an acquisition or divestiture, it’s essential domains are included among the Intellectual Property (IP) assets being purchased. IP assets, including trademarks, patents and copyrights, are often subject to a separate agreement and are typically detailed on a schedule. Buyers should ensure all domains corresponding to any IP asset being purchased are listed on the agreement. Additionally, they should do their own due diligence to ensure brands, misspellings or slogans are not missing. The agreement should also include language prohibiting the seller from registering related domains in the future.

In addition to a detailed schedule, buyers should obtain an acquisition agreement and assignment document from the seller to assist with updating domain ownership. They should work with their domain registrar to file any required documentation with the appropriate registries to transfer and/or update domain ownership.

Once the buyer has the list of domains, he or she should identify the registration date, expiration date and registrar for each domain name. Close attention should be paid to expiration dates to ensure critical domains do not expire.

Acquisition Best Practices

IDENTIFY ALL DOMAIN ASSETS

As mentioned earlier, the purchasing party should request a detailed list of all domain assets included in the acquisition. In addition, it is advised buyers perform their own searches to uncover any missing domains. Using a reverse Whois tool can help identify missing domains using a single data point (company name, name, email, phone number, etc.).

TRANSFER CORE ASSETS AS SOON AS POSSIBLE

Once you have compiled your inventory and identified core, key, important and limited brands, the core domains should be transferred as soon as possible into your domain portfolio to help protect against unintended expiration. This is also a good time to determine if additional locking mechanisms, such as Registry Lock, should be put in place.

CONSOLIDATE AND TRANSFER ALL OTHER ASSETS

Work with your registrar to consolidate any remaining domains into your domain portfolio. Depending on the number of domains being transferred, a transfer plan should be created, and other best practices, including standardizing DNS and Whois contacts, should be followed.

Divestiture Best Practices

IDENTIFY DOMAINS AND MOVE TO NEW ACCOUNT AT EXISTING REGISTRAR

In general, divestitures can be the most difficult to execute. Prior to the close date, work with internal teams and your domain registrar to identify the domains that will be part of the transaction. If the purchasing party does not have an account with your registrar, request an account be opened in the buyer's name. Your registrar may require additional documentation from the buyer to complete this step. On the close date, immediately transfer the domains to the new account. The buyer will need to work with the registrar to ensure domain ownership is properly updated to reflect the new ownership.

Quick Tip

When identifying domains as part of an acquisition or divestiture, use a Reverse Whois tool to help uncover lost domains.

CONCLUSION

Managing an international domain portfolio is an incredibly important part of a global company's overall strategy for protecting its brands and Intellectual Property (IP).

While it is a complex undertaking that includes a number of stakeholders — from internal brand holders and business units to external parties like DNS providers and IP attorneys — working with an experienced, industry-leading, corporate-only domain registrar will provide you the best results in managing this formidable task.

Working in tandem with such a registrar and utilizing the best practices described in this handbook will help you establish an underlying framework for decision making that will result in: improved processes and policies, better resource allocation, access to high quality tools and experts in the field, market-leading security, and a more tightly-focused and flexible domain portfolio.

What started as a way for scientists to communicate has morphed into a means of billions of people communicating and trillions of dollars in sales — the Internet is now the bedrock of the modern business world and managing brands via domain assets is a fundamental requirement of staying competitive and viable as a business. What will happen next? While no one knows exactly, the DNS is sure to continue evolving, and we will be here to help your company evolve along with it.

GLOSSARY

A

Anticybersquatting Consumer Protection Act (ACPA)

ACPA is a United States federal law enacted in 1999 making cybersquatters liable to a civil action if their sole intent is to register a trademark or individual's name for the purpose of reselling the domain to the trademark holder for a profit.

Alternate Dispute Resolution (ADR)

ADR is a catch-all term that describes a number of methods used to resolve disputes out of court, including negotiation, conciliation, mediation and the many types of arbitration. The common denominator of all ADR methods is that they are faster, less formal, cheaper and often less adversarial than a court trial.

Anonymous Acquisition

A domain recovery strategy that involves negotiation through a proxy entity to acquire a target domain.

C

Cache Poisoning

A computer attack where data is introduced into a DNS resolver's cache, causing the name server to return an incorrect IP address, diverting traffic to another website.

Country Code Top-Level Domain (ccTLD)

Two-letter domains, such as .uk (United Kingdom), .de (Germany) and .jp (Japan), are called country code top-level domains (ccTLDs) and correspond to a country, territory or other geographic location. The rules and policies for registering domains in the ccTLDs vary significantly.

Some ICANN-accredited registrars provide registration services in the ccTLDs in addition to registering names in . biz, .com, .info, .name, .net and .org; however, ICANN does not specifically accredit registrars to provide ccTLD registration services.

For more information regarding registering names in ccTLDs, including a complete database of designated ccTLDs and managers, please refer to http://www.iana.org/cctld/cctld.htm.

Cease and Desist (C&D)

A demand to turn over a domain or bring down content based upon pre-existing legal rights.

D

Defensive Registration

This is a domain registration where making a live site is not necessarily desired, but the strategy is more directed towards preventing anyone else from registering the domain.

Domain Name System (DNS)

DNS helps users to find their way around the Internet. Every computer on the Internet has a unique address — just like a telephone number — which is a rather complicated string of numbers. It is called an Internet Protocol (IP) address. IP addresses are hard to remember. DNS makes using the Internet easier by allowing a familiar string of letters (the domain name) to be used instead of the arcane IP address. So instead of typing 207.151.159.3, you can type www.internic.net. It is a mnemonic device that makes addresses easier to remember.

Domain Backorder

A domain service that sends an automated re-registration request to the registry at the moment the domain is deleted.

Domain Name Resolvers

Scattered across the Internet are thousands of computers — called Domain Name Resolvers or just plain resolvers — that routinely cache the information they receive from queries to the root servers. These resolvers are located strategically with Internet service providers (ISPs) or institutional networks. They are used to respond to a user's request to resolve a domain name — that is, to find the corresponding Internet Protocol (IP) address.

G

Generic Top-Level Domain (gTLD)

Most TLDs with three or more characters are referred to as generic TLDs, or generic TLDs, or gTLDs. They can be subdivided into two types: sponsored TLDs (sTLDs) and unsponsored TLDs (uTLDs), as described in more detail below.

In the 1980s, seven gTLDs (.com, .edu, .gov, .int, .mil, .net, and .org) were created. Domains may be registered in three of these (.com, .net, and .org) without restriction; the other four have limited purposes.

Over the following 12 years, various discussions occurred concerning additional gTLDs, leading to the selection in November 2000 of seven new TLDs for introduction. These were introduced in 2001 and 2002. Four of the new TLDs (.biz, .info, .name, and .pro) are unsponsored. The other three new TLDs
(.aero, .coop, and .museum) are sponsored.

Generally speaking, an unsponsored TLD operates under policies established by the global Internet community directly through the ICANN process, while a sponsored TLD is a specialized TLD that has a sponsor representing the narrower community that is most affected by the TLD. The sponsor thus carries out delegated policy-formulation responsibilities over many matters concerning the TLD.

A sponsor is an organization to which some defined ongoing policy-formulation authority regarding the manner in which a particular sponsored TLD is operated is delegated. The sponsored TLD has a charter, which defines the purpose for which the sponsored TLD has been created and will be operated. The sponsor is responsible for developing policies on the delegated topics so that the TLD is operated for the benefit of a defined group of stakeholders, known as the sponsored TLD community, that are most directly interested in the operation of the TLD. The sponsor is also responsible for selecting the registry operator, and to varying degrees, establishing the roles played by registrars and their relationship with the registry operator. The sponsor must exercise its delegated authority according to fairness standards and in a manner that is representative of the sponsored TLD community.

In current terms, sTLDs and pre-2012 application round gTLDs are spoken of in the catchall term of legacy TLDs.

I

Internet Corporation for Assigned Names and Numbers (ICANN)

ICANN is an internationally organized, non-profit corporation that has responsibility for Internet Protocol (IP) address space allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) top-level domain name system management, and root server system management functions. Originally, the Internet Assigned Numbers Authority (IANA) and other entities performed these services under US government contract. ICANN now performs the IANA function. As a private-public partnership, ICANN is dedicated to preserving the operational stability of the Internet; to promoting competition; to achieving broad representation of global Internet communities; and to developing policy appropriate to its mission through bottom-up, consensus-based processes. The DNS translates the domain name you type into the corresponding IP address and connects you to your desired website. The DNS also enables email to function properly, so the email you send will reach the intended recipient.

Internationalized Domain Names (IDNs)

IDNs are domains that include characters used in the local representation of languages that are not written with the 26 letters of the basic Latin alphabet, a-z. An IDN can contain Latin letters with diacritical marks, as required by many European languages, or may consist of characters from non-Latin scripts such as Arabic or Chinese. Many languages also use other types of digits than 0-9. The basic Latin alphabet together with the European-Arabic digits are, for the purpose of domains, termed American Standard Code for Information Interchange (ASCII) characters. These are also included in the broader range of Unicode characters that provides the basis for IDNs.

The hostname rule requires that all domains of the type under consideration are stored in the DNS using only the ASCII characters listed above, with the one further addition of the hyphen (-). The Unicode form of an IDN therefore requires special encoding before it is entered into the DNS.

The following terminology is used when distinguishing between these forms:

A domain name consists of a series of labels (separated by dots). The ASCII form of an IDN label is termed an A-label. All operations defined in the DNS protocol use A-labels exclusively. The Unicode form, which a user expects to be displayed, is termed a U-label. The difference may be illustrated with the Hindi word for test — परीका — appearing here as a U-label would (in the Devanagari script). A special form of ASCII compatible encoding (ACE) is applied to this to produce the corresponding A-label: xn — 11b5bs1di.

A domain name that only includes ASCII letters, digits and hyphens is termed an LDH label. Although the definitions of A-labels and LDH-labels overlap, a name consisting exclusively of LDH labels, such as icann.org is not an IDN.

Internet Protocol (IP)

The communications protocol underlying the Internet, IP allows large, geographically diverse networks of computers to communicate with each other quickly and economically over a variety of physical links. An Internet Protocol Address is the numerical address by which a location in the Internet is identified. Computers on the Internet use IP addresses to route traffic and establish connections among themselves; people generally use the human-friendly names made possible by the DNS.

Internet Service Provider (ISP)

An ISP is a company that provides organizations and/or individuals access to the Internet. Access services provided by ISPs may include web hosting, email, voice over Internet Protocol (VoIP) and support for many other applications.

L

Legacy gTLD

A catchall term that that describes sponsored top-level domains (sTLDs) and pre-2012 application round gTLDs.

Local Presence

A term which describes either an agent or situation where as a prerequisite to registering a ccTLD, the requestor must possess an indigenous local contact. This can include: Business, organization, address, person, or local agent.

M

Malware

An umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, trojan horses, ransomware, spyware, adware, scareware, and other malicious programs.

N

Nameserver

Usually referred to as servers or DNS, nameservers are configured to support a domain name in order for the URL to resolve when entered into a browser.

P

Post-Delegation Dispute Resolution Procedure (PDDRP)

Provides 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).

Pharming

A hacker's attack aiming to redirect a website's traffic to another (bogus) website. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software.

Phishing

Phishing attacks use both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Social engineering schemes use spoofed emails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers.

Hijacking brand names of banks, e-retailers and credit card companies, phishers often convince recipients to respond. Technical subterfuge schemes plant crimeware onto PCs to steal credentials directly, often using Trojan keylogger spyware. Pharming crimeware misdirects users to fraudulent sites or proxy servers, typically through Domain Name System (DNS) hijacking or poisoning.

R

Registrant

The registrant is the owner of a domain name. The owner may be an individual or an organization to whom a specific domain is registered. When a registrant registers a domain and enters a contractual agreement with the registrar, they are the legal owner of a domain for a specific period of time.

Registrar

Domain names are registered through many different companies known as registrars. MarkMonitor, for example, is an ICANN-accredited registrar with an exclusive focus on corporate domain portfolios. A complete listing of registrars is in the Accredited Registrar Directory.

A registrar asks individuals, or registrants, various contact and technical information that make up the registration. The registrar maintains records of the contact information and submits the technical information to a central directory known as the registry. The registry provides other computers on the Internet the information necessary to send the registrant email or to find the registrant's website.

Registry

The registry is the authoritative, master database of all domains registered in each top-level domain (TLD). The registry operator keeps the master database and also generates the zone file, which allows computers to route Internet traffic to and from top-level domains anywhere in the world. Internet users don't interact directly with the registry operator; users can register names in TLDs including .biz, .com, .info, .net, .name, .org by using an ICANN-accredited registrar.

Root Servers

The root servers contain the Internet Protocol (IP) addresses of all the top-level domain (TLD) registries — both the global registries such as .com, .org, etc. and the 244 country-specific registries such as .fr (France), .cn (China), etc. This is critical information. If the information is not 100% correct or if it is ambiguous, it might not be possible to locate a key registry on the Internet. In Domain Name System (DNS) parlance, the information must be "unique and authentic."

Registry Restriction Dispute Resolution Procedure (RRDRP)

A complaint procedure for community-based generic top-level domains (gTLDs). 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.

S

Site/Website

A set of related web pages typically served from a single web domain.

Social Engineering

Social engineering schemes use spoofed emails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers.

T

Top Level Domain (TLD)

TLDs are the names at the top of the DNS naming hierarchy. They appear in domains as the string of letters following the last (rightmost) dot, such as "net" in www.example.net. The administrator for a TLD controls what second-level names are recognized in that TLD. The administrators of the root domain or root zone control what TLDs are recognized by the DNS. Commonly used TLDs include .com, .net, .edu, .jp, .de, etc.

U

Uniform Dispute Resolution Policy (UDRP)

All ICANN-accredited registrars follow a uniform dispute resolution policy. Under that policy, disputes over entitlement to a domain name registration are ordinarily resolved by court litigation between the parties claiming rights to the registration. Once the courts rule who is entitled to the registration, the registrar will implement that ruling. In disputes arising from registrations allegedly made abusively (such as cybersquatting and cyberpiracy), the uniform policy provides an expedited administrative procedure to allow the dispute to be resolved without the cost and delays often encountered in court litigation. In these cases, you can invoke the administrative procedure by filing a complaint with one of the dispute-resolution service providers.

Uniform Rapid Suspension (URS)

The URS was designed to provide a cost-effective, expedited process to address issues of trademark infringement and abuse. Domains are suspended in the DNS for the remainder of the registration term but will be available again for registration once the domain expires.

W

Whois

Whois (pronounced "who is;" not an acronym) is an Internet protocol used to query databases to obtain information about the registration of a domain name (or Internet Protocol (IP) address). The WHOIS protocol was originally specified in RFC 954, published in 1985. The current specification is documented in RFC 3912. ICANN's generic top-level domain (gTLD) agreements require registries and registrars to offer an interactive web page and a port 43 Whois service providing free public access to data on registered names. Such data is commonly referred to as Whois data, and includes elements such as the domain registration creation and expiration dates, nameservers and contact information for the registrant and designated administrative and technical contacts.

Whois services are typically used to identify domain holders for business purposes and to identify parties who are able to correct technical problems associated with the registered domain.

ICANN and Community-Related Definitions

A

Advisory Committee

An Advisory Committee is a formal advisory body made up of representatives from the Internet community to advise ICANN on a particular issue or policy area. Several are mandated by the ICANN Bylaws and others may be created as needed. Advisory committees have no legal authority to act for ICANN, but report their findings and make recommendations to the ICANN Board.

African Network Information Center (AfriNIC)

AfriNIC is a Regional Internet Registry (RIR), and is a non-profit membership organization responsible for the administration and registration of Internet Protocol (IP) addresses in the Africa region.

At-Large Advisory Committee (ALAC)

ICANN's ALAC is responsible for considering and providing advice on the activities of the ICANN as they relate to the interests of individual Internet users (the at-large community). ICANN, as a private sector, non-profit corporation with technical management responsibilities for the Internet's domain name and address system, will rely on the ALAC and its supporting infrastructure to involve and represent in ICANN a broad set of individual user interests.

On 31 October 2002, the ICANN Board adopted new bylaws that establish the ALAC and authorize its supporting at-large organizations (Article XI, Section 2(4) of the new bylaws). The new bylaws, which are the result of ICANN's 2002 reform process, went into effect on December 15, 2002. ALAC will eventually consist of 10 members selected by regional at-large organizations, supplemented by five members selected by ICANN's Nominating Committee. To allow the ALAC to begin functioning immediately, the Transition Article of the Interim Bylaws provides for the board to appoint 10 members (two from each of ICANN's five regions) to an interim ALAC.

Underpinning the ALAC will be a network of self-organizing, self-supporting at-large structures throughout the world involving individual Internet users at the local or issue level. The at-large structures (either existing organizations or newly formed for this purpose) will self-organize into five regional at-large organizations (one in each ICANN region — Africa, Asia-Pacific, Europe, Latin America/Caribbean and North America). The regional at-large organizations will manage outreach and public involvement and will be the main forum and coordination point in each region for public input to ICANN.

Asia Pacific Network Information Centre (APNIC)

APNIC is a regional Internet registry (RIR) and is a non-profit membership organization responsible for the administration and registration of Internet Protocol (IP) addresses in the Asia-Pacific region, including Japan, Korea, China and Australia.

American Registry for Internet Numbers (ARIN)

ARIN is a regional Internet registry (RIR) and is a non-profit membership organization established for the purpose of the administration and registration of Internet number resources — including Internet Protocol (IP) addresses and Autonomous System Numbers — in Canada, many Caribbean and North Atlantic islands and the United States. ARIN also develops consensus-based policies and facilitates the advancement of the Internet through information and educational outreach.

Address Supporting Organization (ASO)

The ASO advises the ICANN Board of Directors on policy issues relating to the allocation and management of Internet Protocol (IP) addresses. The ASO selects two directors for the ICANN board.

C

Country-Code Names Supporting Organization (ccNSO)

ccNSO is a body within the ICANN structure created for and by ccTLD managers. Since its creation in 2003, the ccNSO has provided a forum for country code top-level domain (ccTLD) managers to meet and discuss topical issues of concern to ccTLDs from a global perspective. The ccNSO provides a platform to nurture consensus, technical cooperation and skill building among ccTLDs, and facilitates the development of voluntary best practices for ccTLD managers. It is also responsible for developing and recommending global policies to the ICANN board for a limited set of issues relating to ccTLDs, such as the introduction of Internationalized Domain Name ccTLDs (IDN ccTLDs). Membership in the ccNSO is open to all ccTLD managers responsible for managing an ISO 3166 country-code top-level domain.

G

Governmental Advisory Committee (GAC)

The GAC is an advisory committee comprised of appointed representatives of national governments, multi-national governmental organizations and treaty organizations, and distinct economies. Its function is to advise the ICANN board on matters of concern to governments. The GAC will operate as a forum for the discussion of government interests and concerns, including consumer interests. As an advisory committee, the GAC has no legal authority to act for ICANN, but will report its findings and recommendations to the ICANN board. The chairman of the GAC is Heather Dryden of Canada.

Generic Names Supporting Organization (GNSO)

The GNSO is the successor to the responsibilities of the Domain Name Supporting Organization (see “DNSO” below) that relates to the generic top-level domains.

The GNSO is the body of six constituencies, as follows: the Commercial and Business constituency, the gTLD Registry constituency, the ISP constituency, the non-commercial constituency, the registrar’s constituency, and the IP constituency.

I

Internet Assigned Numbers Authority (IANA)

IANA is the authority originally responsible for the oversight of Internet Protocol (IP) address allocation, the coordination of the assignment of protocol parameters provided for in Internet technical standards, and the management of the Domain Name System (DNS), including the delegation of top-level domains and oversight of the root nameserver system. Under ICANN, the IANA continues to distribute addresses to the Regional Internet Registries, coordinate with the Internet Engineering Task Force (IETF) and others to assign protocol parameters, and oversee the operation of the DNS.

Internet Engineering Task Force (IETF)

The IETF is a large open international community of network designers, operators, vendors and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual.

Internet Society (ISOC)

ISOC is the international organization for global cooperation and coordination for the Internet and its internetworking technologies and applications. ISOC membership is open to any interested person.

L

Latin American and Caribbean Internet Addresses Registry (LACNIC)

LACNIC is a regional internet registry (RIR) and is a non-profit membership organization responsible for the administration and registration of Internet Protocol (IP) addresses for Latin America and the Caribbean.

O

Operations Steering Committee (OSC)

The OSC coordinates, recommends and reviews changes to certain operational activities of the Generic Names Supporting Organization (GNSO) and its constituencies with a view to efficient outcomes. These operational activity areas cover GNSO operations, stakeholder group and constituency operations, and communications with GNSO and between GNSO and other ICANN structures.

P

Policy Development Process (PDP)

The PDP is a set of formal steps, as defined in the ICANN to guide the initiation, internal and external review, timing and approval of policies needed to coordinate the global Internet's system of unique identifiers.

Policy Process Steering Committee (PPSC)

The PPSC reviews and recommends processes used within the GNSO for developing policy, including the use of Working Groups, and recommending any changes.

R

Registry Services Evaluation Process (RSEP)

Problems and complaints relating to deletion of domain-name registrations are very common. Businesses and consumers are losing the rights to their domains through registration deletions caused by mistake, inadvertence or fraud. Current procedures for correcting these mistakes have proven inadequate. To move toward a solution to these problems ICANN developed the RGP.

How it works: Now, the "delete" of a domain name (whether inside or outside of any applicable grace period) will result in a 30-day Deleted Name Redemption Grace Period. This grace period will allow the domain name registrant, registrar and/or registry time to detect and correct any mistaken deletions.

During this 30-day period, the deleted name will be placed on REGISTRY-HOLD, which will cause the name to be removed from the zone. (The domain name will not function or resolve.) This feature will help ensure notice to the registrant that the name is subject to deletion at the end of the RGP, even if the contact data the registrar has for the registrant is no longer accurate.

During the RGP, registrants can redeem their registrations through registrars. Registrars redeem the name in the registry for the original registrant by paying renewal fees, plus a service charge, to the registry operator. Any party requesting redemption would be required to prove its identity as the original registrant of the name.

After the 30-day period, there is a five-day period when the domain essentially is pending deletion. This timeframe is implemented to facilitate notice to all registrars before a domain is finally deleted.

Réseaux IP Européens (RIPE) and RIPE NCC

RIPE is an open and voluntary organization that consists of European Internet service providers. The RIPE NCC acts as the regional internet registry (RIR) for Europe and surrounding areas, performs coordination activities for the organizations participating in RIPE, and allocates blocks of Internet Protocol (IP) address space to its local Internet registries (LIRs), which then assign the addresses to end-users.

Regional Internet Registry (RIR)

There are currently five RIRs: African Network Information Center (AfriNIC), Asia Pacific Network Information Centre (APNIC), American Registry for Internet Numbers (ARIN), Latin American and Caribbean Internet Addresses Registry (LACNIC) and Réseaux IP Européens (RIPE) NCC. These non-profit organizations are responsible for distributing and managing Internet Protocol (IP) addresses on a regional level to Internet service providers and local registries.

S

Security, Stability and Resiliency (SSR)

In ICANN's SSR Framework, security means the capacity to protect and prevent misuse of Internet unique identifiers. Stability means the capacity to ensure the system operates as expected, and users of the unique identifiers have confidence that the system operates as expected. Resiliency means the capacity of the unique identifier system to effectively withstand, tolerate or survive malicious attacks and other disruptive events without disruption or cessation of service.

Supporting Organizations (SO)

The SOs are the three specialized advisory bodies that will advise the ICANN board of directors on issues relating to domains — Generic Names Supporting Organization (GNSO) and Country Code Names Supporting Organization (CCNSO) — and Internet Protocol (IP) addresses — Address Supporting Organization (ASO).

Security and Stability Advisory Committee (SSAC)

SSAC is the ICANN Board President's standing committee on the security and stability of the Internet's naming and address allocation systems. Their charter includes a focus on risk analysis and auditing. SSAC consists of approximately 20 technical experts from industry and academia as well as operators of Internet root servers, registrars and top-level domain (TLD) registries.

U

Unique Identifier Health

In ICANN's Security, Stability and Resiliency Framework, "unique identifier health" means a state of general functioning of the Internet's unique identifiers that is within nominal technical bounds in the dimensions of coherency, integrity, speed, availability, vulnerability and resiliency.

W

World Wide Web Consortium (W3C)

The W3C is an international industry consortium founded in October 1994 to develop common protocols that promote the evolution of the World Wide Web and ensure its interoperability. Services provided by the W3C include: a repository of information about the World Wide Web for developers and users, reference code implementations to embody and promote standards, and various prototype and sample applications to demonstrate use of new technology.

World Intellectual Property Organization (WIPO)

WIPO is an intergovernmental organization based in Geneva, Switzerland responsible for the promotion of the protection of intellectual rights throughout the world. It is one of the 16 specialized agencies of the United Nations system of organizations.

About MarkMonitor

MarkMonitor, the leading enterprise brand protection solution and a Clarivate Analytics flagship brand, provides advanced technology and expertise that protects the revenues and reputations of the world's leading brands. In the digital world, brands face new risks due to the Web's anonymity, global reach and shifting consumption patterns for digital content, goods and services. Customers choose MarkMonitor for its unique combination of advanced technology, comprehensive protection and extensive industry relationships to address their brand infringement risks and preserve their marketing investments, revenues and customer trust. For more information, visit **markmonitor.com**.

About Clarivate Analytics

Clarivate Analytics accelerates the pace of innovation by providing trusted insights and analytics to customers around the world, enabling them to discover, protect and commercialize new ideas faster. Formerly the Intellectual Property and Science business of Thomson Reuters, we own and operate a collection of leading subscription-based services focused on scientific and academic research, patent analytics and regulatory standards, pharmaceutical and biotech intelligence, trademark protection, domain brand protection and intellectual property management. Clarivate Analytics is now an independent company with over 4,000 employees, operating in more than 100 countries and owns well-known brands that include Web of Science, Cortellis, Thomson Innovation, Derwent World Patents Index, CompuMark, MarkMonitor and Techstreet, among others. For more information, visit **clarivate.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) 207 433 4000
www.markmonitor.com

MarkMonitor
Protecting brands in the digital world

Clarivate
Analytics