



WHITE PAPER

---

# Protecting and Managing Your Company's Online Identity

Strategic Solutions for Corporate Domain  
Name Challenges



Where it all comes together.™

**CONTENTS**

+ Executive Summary	3
+ The Challenges	4
+ Planning Your Strategy	5
+ Nine Steps to a Successful Domain Name Strategy	7
Step 1: Identify and Rank Assets	7
Step 2: Consolidate Existing Domain Name Registrations	7
Step 3: Establish Standards and Procedures	7
Step 4: Align Portfolio with Current Standards and Procedures	8
Step 5: Execute a Strategy to Register Domain Names	8
Step 6: Recover Names	9
Step 7: Manage and Monitor Your Portfolio	9
Step 8: Monitor and Protect Your Assets	10
Step 9: Use Brand Assets to Generate Revenue	10
+ Case Studies: Corporate Domain Name Problems	11
Case 1: The Cost of Failing to Renew a Name	11
Case 2: Setting Up Proper Standards and Procedures	12
+ Top-Level Domains	12
Generic Top-Level Domains (gTLDs)	12
Country-Code Top-Level Domains (ccTLDs)	14
New Proposed Sponsored Top-Level Domain (sTLDs)	17
Using ccTLDs to Improve Customer Satisfaction and Drive Revenue	18
+ Internationalized Domain Names	18
+ VeriSign Digital Brand Management Services	19



## Executive Summary

Most companies recognize that domain names are the essential means of establishing brand identity on the Internet, and therefore, are among a company's most valuable business assets. Failure to secure and protect domain names puts one of a company's most important communications and revenue channels—and its brand identity—at risk.

On the other hand, securing domain names that reflect the company's brand, services, or products can drive traffic, sales, and revenue. For companies with a global presence, managing an international domain name portfolio is a critical and increasingly complex challenge. Selecting and implementing a sound strategy and reliable management system is the long-term key to maintaining a portfolio with a minimum of risk and aggravation. Staying informed allows companies to adjust their strategy as the need arises. Thinking ahead, beyond protection, allows companies to turn valuable brand assets from a cost center to an effective generator of sales and revenue.

### The Challenges

The challenges that intellectual property owners face have been well documented in the press and in professional publications. Legal and regulatory solutions have been implemented. Nonetheless, the problems remain real and expensive to resolve.

### Planning and Implementing a Strategy

Managing brands on the Internet is complex. Changing plans mid-stream can be frustrating and costly. Implementing a sound long-term strategy based on current and projected needs is the best way to protect a brand. This guide includes a proven nine-step method, used by VeriSign's most successful customers, for controlling brand assets and using them to profit.

### Portfolio Management

As the domain name industry matures, and as companies expand, review, and refine their portfolio, portfolio management will be the key to effective brand protection. The capability of domain name vendors' technology will become more important as the need increases for instant information and visibility into the portfolio.

### Staying Informed

Effective management includes getting timely information and strategic advice so managers can make prudent plans well ahead of any crisis, revise their strategy as necessary, and keep management tasks routine and under control. This guide outlines some of the areas where uncertainty and change can pose risks to the enterprise's strategy.

### Beyond Protection

Although the focus of many companies and domain name vendors has been to protect their brands in the domain name space, future attention will shift to using domain names to generate Web traffic, sales, and revenues. Some less savory groups of domain name registrants, including "typosquatters" and traffic thieves, have, despite their objectionable motives, shown that registration of selected domain names is an effective method of leading qualified prospective customers to a Web site. Some companies have already embarked on successful "offensive" registration campaigns, in which they have registered not only generic domain names describing their products but also misspellings of their brand names to

## THE ROLE OF ICANN

ICANN is a non-profit, technical coordination body for the Internet. Created in October 1998 by a broad coalition of the Internet's business, technical, academic, and user communities, ICANN is responsible for a set of technical functions previously performed under U.S. government contract by the Internet Assigned Names Authority (IANA) and other entities. Specifically, ICANN coordinates the assignment of the Internet domain names, Internet Protocol (IP) address numbers, and protocol parameter and port numbers.

The U.S. Department of Commerce agreed to a joint agreement with ICANN to extend its Memorandum of Understanding (MOU) until September 30, 2006. The new MOU includes a number of milestones for ICANN and related deadlines, such as creating a strategic plan to support key DNS management tasks in the long term; working with the Commerce Department to guarantee that ICANN's corporate organizational documents back privatization of DNS technical management; forming relationships with root server system operators; working out processes to improve transparency and accountability in terms of DNS technical management; developing agreements with ccTLD operators; creating a new plan for choosing new TLDs; bettering accuracy of WHOIS data; and developing ways to encourage Internet communities to participate in ICANN.

drive more traffic and sales. In addition, many companies are now adopting proactive brand monitoring solutions.

### Summary

Knowing where and how to protect your company's identity online is critical to business. Because the domain name environment is always changing, simply registering a company's name and brands is not enough to protect its identity. A program of long-term monitoring and management is also critical to your business or organization. Whether you manage domain names in house, use an outside vendor, or use a combination of the two, the growing complexity of a successful brand asset strategy requires careful planning and a well-managed implementation.

## The Challenges

The challenges facing intellectual property owners on the Internet are well known. Online brand abuse has spawned legislation in many countries, and many law firms have domain name specialists. One of the first acts of the Internet Corporation for Assigned Names and Numbers (ICANN), the international domain name regulatory body, was to enact the Uniform Dispute Resolution Policy (UDRP), which incorporates procedures for registrars, trademark holders, and individuals to address abuses. The problems are becoming better understood and more manageable, but they remain very real and widespread.

Although the issues have been well publicized, most medium and large enterprises do not have a comprehensive global domain name strategy. As a result, they must contend with increased risk of identity theft, intellectual property infringement, and loss of revenue streams associated with their brands. In addition, an increasing number of companies have become victim to online fraud schemes, such as "phishing" attacks, in which criminals use email addresses and Web sites that mimic well-known companies to get users to divulge personal and financial data. Despite the decision by many companies to pursue only the most egregious violations, the combined cost of infringement, lost revenue, customer dissatisfaction, and legal expenses remains very high. Proactively acquiring your major digital brand assets is more practical and more profitable than attempting to litigate or recover them when infringement is discovered.

Complexity is the main obstacle to meeting the challenges. Consider all the domain names and variations registered for your company and its products, services, trademarks, and brands. Besides the brand names your company currently uses, consider the domain names it may want to use for upcoming products and services or prevent others from using.

Now, think about all of the countries in which the company conducts business now and potentially in the future. Although *.com* is still the most popular extension, country-code top-level domains (ccTLDs) account for 39 percent of all top-level domain (TLD) registrations. Many countries have a variety of restrictions on who can register and use domain names, and some offer no protection if someone else registers your name. In addition, an internal survey of ccTLD registries shows that up to 20 percent of country registration requirements may change on a quarterly basis, making it even more difficult to stay up-to-date with what is needed to submit a registration request.

## IS YOUR COMPANY ADEQUATELY PREPARED?

Is your company effectively managing and protecting its registered domain names? With the addition of newer gTLDs and the increased prominence of ccTLDs such as *.us* and *.de*, is your company sufficiently protected?

Many companies cannot answer these basic questions:

- How many domain names does your company control?
- Who is responsible for maintaining each of these domain names? Is a central person responsible for coordinating and managing all your company's domain names? What will happen if that person leaves the company or forgets to pay the renewal bill?
- Do you have a crisis plan to recover domain names if someone uses your brand names without your knowledge?
- Do you have a strategy for registering and maintaining domain names in the unrestricted Internet domains that do not subscribe to the ICANN dispute policy?
- Do you have a strategy to register new TLDs?
- Do you have any technology or procedures to monitor how partners and distribution channels use your domain names and brands?
- Are you aware of recent developments in IDNs that could impact your business?
- Where do your names resolve—or do they even resolve? If prospective customers type your company name or one of your products into a search engine or Web browser, are you sure they'll reach your Web site?

If you cannot answer these questions, you need to develop a strategy to protect and manage your company's domain name portfolio.

Even among generic top-level domains (gTLDs) there are a variety of domain name options—*.com*, *.org*, and *.net*, as well as newer gTLDs such as *.biz*, *.info*, *.pro*, and *.name*. Finally, there are Internationalized Domain Names (IDNs), which use non-English character sets, and the new “sponsored TLDs” (sTLDs) that ICANN is considering for approval, such as *.travel* and *.mobi*.

The external threats to a company's domain names also continue to multiply. They include the following:

- Speculators registering variants of a company's name, hoping to resell them back to the company.
- Speculators monitoring domain names, hoping the company inadvertently allows them to expire, and then registering them and attempting to sell them back to the company.
- Critics who register a domain name similar to the company's name to make disparaging remarks or create public awareness of potentially damaging information.
- Traffic diverters who register the company's brand names (or variations of them) in order to redirect customers looking for the company's products and services to another site—or to lure unwitting customers into divulging critical personal information and financial data.
- People with no malicious intent who coincidentally register a domain name the company wants. This is of particular concern if someone anywhere else in the world legitimately uses the same name as the company or brand name.

Failure to protect domain names from deletion, hijacking, or cybersquatting often results in complex and expensive recovery operations, which typically cost much more than a well-planned domain name strategy.

## Planning Your Strategy

As your company's Internet usage and presence grows, so will its inventory of domain names. Managing new and existing domain names with multiple renewal dates and contracts—and turning them into digital brand assets and promotional tools—is a complex task.

First, you need to answer the following questions:

- How do you protect your primary and secondary brands and trademarks from unauthorized use on the Internet?
- How do you identify, consolidate, and manage all the domain names that have been registered on behalf of the company—including those registered by former employees or foreign offices?
- How should your strategy deal with the oddities of the domain name landscape? How do you evaluate gTLDs compared to ccTLDs? Restricted versus unrestricted domains? IDNs versus ccTLDs?
- How do you meet local presence requirements so you can register a domain name in a restricted country?
- How can you balance legal, marketing, and technical needs with budget constraints?

## WHAT IS A CORPORATE DOMAIN NAME MANAGER?

An emerging role within enterprise companies is that of the corporate domain name manager. Although the domain name manager may come from the marketing, legal, or IT department, this person generally has an advanced understanding of the entire organization's technical and business needs and seeks to meet them by establishing and enforcing policies and procedures on a company-wide basis.

Corporate domain name managers generally seek to work with all the stakeholders in developing a brand management strategy, thereby ensuring buy-in from all business unit managers.

Besides leading strategy development and implementation, the corporate domain name manager's job includes the following responsibilities:

- Staying abreast of registration and renewal requirements
- Updating the portfolio on a regular basis with registrations for new domain names, products, services, and trademarks
- Evaluating unused names
- Tracking registration and Internet usage trends to make registration recommendations
- Monitoring and approving changes to Domain Name System (DNS), contact, and registrant information
- Monitoring for brand misuse or abuse
- Providing business units with centralized reporting on domain name portfolios, including spending levels, pricing, and implementation timeframes

Corporate domain name managers can also play an important role in mergers and acquisitions by helping to identify existing online assets for the companies in question and flagging any domain name ownership issues early in the process.

- What are the consequences (and potential costs and liabilities) if you do not protect your company and brand names in all the unrestricted gTLDs, the unrestricted ccTLDs, and restricted ccTLDs?
- Can you centralize the management of your portfolio of digital assets online yet still allow multiple designated employees to access and manage only the names important to their division or department?
- What domain names should you register to increase the promotion and sales of products online? How can you use existing domain registrations to generate more revenue? Are you missing revenue opportunities by not registering names in certain markets?
- How do you handle the logistics of renewing names? Where do you find the expertise in multiple foreign languages? How do you pay in multiple currencies? How do you keep track of what renewals are due and when?
- How do you start?

Once you have assessed the current situation, you need to prioritize your brands, services, and products.

You may need to perform the following tasks:

- Designate an individual (or several individuals) who will be responsible for managing the domain name portfolio.
- Identify all the domain names the company controls, including those that may be registered by other business divisions within the company or outside your country.
- Identify the brands, trademarks, and variations you wish to register as domain names.
- Establish and manage an organized, long-term plan to register domains as promotional tools for new products and services.
- Create an action plan to be used in the event a competitor or cybersquatter registers a domain name that is valuable to the company. Plans may vary depending on whether the company is registering a domain in a gTLD or in a ccTLD that does not subscribe to the ICANN dispute policy.
- Determine whether existing and upcoming company products and services are correctly registered in the regions where the company does business. In this exercise you should also examine language and alphabet differences.

# Nine Steps to a Successful Domain Name Strategy

VeriSign® Digital Brand Management Services recommends a nine-step strategy towards gaining control of your domain names. Every company is different, but, in broad strokes, following these steps will ensure that you maintain control of your brand assets on the Internet. These steps may be generally described as auditing, standards setting, modifications management, and revenue generation.

## + Step 1: Identify and Rank Assets

Identify and order your brand assets into the following ranks:

- Critical
- Important
- Secondary (which includes trademarks, brands, slogans, other named intellectual property, and other names)

Some brands are critical; some are important in certain regions, but not in others; secondary assets include names of key executives, new products and services (including those that are not yet launched), and generic names that describe what you sell. Rank all assets, and assign a value to them in each region where you do business.

## + Step 2: Consolidate Existing Domain Name Registrations

Consolidate all your existing domain name registrations into a single managed account.

- Work with a registrar or an in-house specialist to help “find” your existing gTLD registrations. This can be done by searching the WHOIS database of domain name registrant information. You can search the database by registrant name, Network Information Center (NIC) contact handle, Domain Name System (DNS), email address, and phone number. Search ccTLD WHOIS databases to get an understanding of country-code names in your control.
- Lock in gTLD registrations with your registrar. This will eliminate unplanned and unauthorized deactivations and modifications, as well as unauthorized gTLD transfers.

## + Step 3: Establish Standards and Procedures

Set up standards and procedures across the company as a whole.

- Identify the preferred administrative contact. Usually a “role” is preferable to an actual person. Set up company-controlled email aliases (such as [admin@companyxyz.com](mailto:admin@companyxyz.com)) as necessary so that someone is always able to receive important communications.
- Identify the preferred name servers and collect technical information. Determine which individuals in the company may register names.
- Determine who will be permitted to approve orders for new domain names, renewals, and modifications.

- Determine where you want domain names to “point.” If an Internet user types in one of your domain names, where do you want that user to go? For example, think about matching foreign-language domain names to language-specific Web sites. You may wish to outsource your DNS to a trusted DNS management vendor so you can easily make changes.
- Either implement these standards and procedures in your in-house software, or find a vendor who can provide these services for you.

#### + Step 4: Align Portfolio with Current Standards and Procedures

Modify your current domain name portfolio to match specifications established by your standards and procedures.

- Review each domain name to ensure that it meets your standards, and that the contact information has been updated. Modify registrant or contact information as necessary.
- In the case of ccTLDs that have special requirements (e.g., requiring the listed administrative contact to be located within the country), modify information to reflect as much common contact information as possible.

#### + Step 5: Execute a Strategy to Register Domain Names

Concurrent with Step 4, execute a strategy to register any domain names that should have been registered but were not.

Ensure that all applications meet individual domain registry requirements. You or your service provider will need to perform the following tasks:

- Prepare applications. Many ccTLDs have special requirements. You may need to supply an in-country address, prove that you have a business in the country, or supply proof of a trademark in the country.
- Set up your DNS. Failure to properly set up primary and secondary host name servers is a common reason for having applications rejected by ccTLDs.
- Submit applications in the format required by the registry in question: HTML, email, or fax.
- Pay fees according to the registry’s procedures.

Your company probably has registered quite a few domain names already. Consider registering important names in the following priority order:

1. Unrestricted gTLDs (e.g., *.com*, *.net*, *.org*, *.info*, *.name*, and *.biz*)
2. Unrestricted ccTLDs (e.g., the United Kingdom, Denmark, and Mexico)
3. Restricted ccTLDs (e.g., the United States, Germany, Sweden, France, China, Korea, and Japan)
4. Restricted gTLDs (e.g., *.pro*, *.coop*, *.aero*, and *.museum*)
5. IDNs (e.g., domain names that use non-English character sets)

Depending on your company’s situation, it may be necessary to rearrange these priorities, particularly if the company is actively doing business or promoting products and services in the restricted ccTLDs.

### + Step 6: Recover Names

Recover names that have been registered by cybersquatters or other individuals.

Several methods are available: By using either local laws and courts or ICANN's UDRP, you may be able to recover names illegitimately registered by another party. If the UDRP or legal proceedings (and related publicity) are unattractive or inappropriate, however, anonymous acquisition may be preferable. Costs for various recovery methods will vary depending on the dispute resolution process (or lack thereof) and the particular domain name under consideration.

### + Step 7: Manage and Monitor Your Portfolio

Manage and monitor your portfolio going forward. With many domain names in the company portfolio, you will need to modify records occasionally.

The following list identifies some events that will require your attention:

- Mergers and acquisitions
- New product or service development
- Market development or introduction of products and services into a specific country
- New servers or security arrangements
- Transfer or termination of key employees
- Billing and budget issues
- Departmental or project billing requirements
- Address changes

You will also need to present reports on the portfolio to the legal, marketing, and technology departments. Either your in-house software, or that of your vendor, should include an easy method or system to manage the domain name portfolio.

The software should allow you to perform the following tasks:

- Search and submit registrations in the high-risk gTLDs and ccTLDs.
- Access the company's domain name portfolio data from a secure, central online location.
- Audit and track orders that have been placed.
- Give many users access to the system, with the capability to give certain users specific permissions to order, modify, or view the portfolio.
- Make registration and modification requests from the company's internal users subject to approval by appropriate persons or departments (e.g., from the legal department).
- Search for domain names flexibly and comprehensively.
- Produce a wide variety of reports to suit internal reporting needs.
- Allocate costs to the appropriate departments within the company.
- Obtain regular action reports to track the status of orders.

## WHAT IS DNS ASSURANCE?

A reliable DNS is essential for companies doing business online. The DNS allows people to use names (e.g., *www.verisign.com*) rather than Internet Protocol (IP) addresses (such as 65.205.249.60) to find Web sites and send email. When a user types *www.verisign.com* into a Web browser, for example, a behind-the-scenes process quickly translates the name into an IP address, which is passed to the Web browser so that it can connect to the intended Web site. This process, called resolution, relies on a global network of name servers operated by many different companies and organizations.

When portions of the network that manage a particular company's domain name break, the effects can be severe and widespread. Without a well-configured, robust DNS, companies can lose access to their email and Web sites, and therefore potentially lose millions of dollars in lost productivity and revenue. The increased use of the Internet for mission-critical operations has brought this issue to the forefront.

The process of large-scale DNS management is complex. Typically, DNS tools are home-grown and difficult to use. All too often, errors occur that are hard to detect or troubleshoot. Staying up-to-date on the latest advances in technology requires significant time.

Due to the cost and complexity of implementing a robust and distributed DNS management solution in house, many enterprises host all their domain names on a single set of servers. If these servers become unavailable for any reason—human error, physical or virtual attack, or natural disaster—the company's Web sites, email, and other Internet services will become unavailable.

## + Step 8: Monitor and Protect Your Assets

Once the company has established domain name procedures, recovered missing names, and registered available names to fill gaps in the portfolio, you—or a trusted third party—must monitor and protect your assets. Online brand monitoring services can find infringing Web sites even if they are not using your brand in their domain names.

These services should be able to perform the following functions:

- Utilize data collection, categorization, and filtering tools to identify sites that infringe on branding, present brand distribution opportunities, or require brand renaming.
- Establish a reporting schedule, priorities, and procedures to effectively deal with infringing sites.
- Utilize data gathering to identify new revenue opportunities and prevent lost revenue.
- Determine which brands should be registered in countries that require some form of local presence (i.e., as a local tax ID number, local or regional trademark, local administrative or billing contact, or in-country DNS servers).
- Establish local administrative, billing, and technical contacts, and in-country DNS hosting, if required, to qualify for registration in restricted countries.

## + Step 9: Use Brand Assets to Generate Revenue

It is not enough to have a domain name portfolio that is properly managed, monitored, and protected. Digital brand assets represent a significant investment, and they can help you make money if you put them to use.

The best way to get a return on your investment is to make sure that your domain name registrations go directly to one of your Web sites instead of a “parked” or “under construction” Web page. It should be easy for customers to find you online. For example, domain name registrations for the French market should point to a Web site in French. Product or service names that you registered as domain names should direct users to the appropriate pages within your Web site.

Strategize where you want your domain name registrations to point. Then either work with the technical department to write scripts and modify DNS entries as necessary, or work with an outsourced service to execute the changes. Qualified prospects will now have many ways to find you.

Unfortunately, most companies do not recognize the weaknesses in their existing DNS infrastructure until it is too late and they have suffered lost productivity or revenue. VeriSign estimates that business losses due to DNS failures may exceed \$1 billion a year due to lost sales, poor customer experiences, and missed or delayed communications.

There are several solutions to the problem of DNS management. One is to rely upon your Internet service provider or Web hosting company. Another is to manage the DNS in house, which requires an expert, on-call staff and significant, ongoing investment in technology and equipment. A third option is to leverage VeriSign® DNS Assurance Services, which can provide a simple, reliable means to ensure 100 percent performance. DNS Assurance Services can also help companies manage their in-house DNS.

Whether a company chooses to outsource management or keep it in house, it should carefully consider the DNS and its implications for Web site accessibility. Maintaining a Web site that is always accessible is a key component to building a strong brand identity.

## Case Studies: Corporate Domain Name Problems

Real-life case studies demonstrate domain name registration challenges in protecting a company's identity on the Internet.

### + Case 1: The Cost of Failing to Renew a Name

A well-established global financial services company neglected to pay a \$35 renewal bill for its main .com domain name. The company's name is heavily advertised and its Web site generates millions of dollars of revenue each month. The domain registrar performed its obligations by attempting to notify the company on several occasions to pay the bill. (Domain names are similar to phone numbers; the name is in service as long as the registrant's account is not in default.) Eventually the domain registrar deactivated the domain name.

When a domain name is deactivated, it no longer sends traffic to the customer-designated IP address, resulting in the display of blank pages or error messages when customers attempt to browse the site. Such was the case for the company.

The company's technical and e-commerce staff was unable to determine the cause of its global dilemma until someone discovered that the company had failed to pay a domain name renewal invoice.

The company lost hundreds of thousands of dollars in revenue and new customer opportunities, and had to battle adverse press. The problems mounted when the company realized that it had many additional domains that needed to be renewed.

Failure to renew is the most common reason for involuntary domain name deactivation. Speculators now use powerful tools that automate the monitoring of domain names slated for deletion. If a company neglects to renew a name, a speculator can register the name as soon as it is dropped, further compounding the problem.

The domain name registrant organization is responsible for maintaining proper contact information for the registrant, billing, administrative, and technical contacts. This task can be challenging if the company has registered numerous domain names. It is not unusual for several different employees or departments to register domain names for their company, often using different and non-standard addresses, departments, and email contact addresses for each domain.

For example, the marketing group may register new service or product name ideas, an advertising agency may register a promotional event name, and the legal department may register corporate trademarks. Some employees may even register critical company names in their own name, or use their own name for billing or administrative contacts. Lack of a registration policy can easily result in unplanned deactivations and lost names, often leaving the company with little control over its key domain registrations, as is illustrated in the following case study.

### + Case 2: Setting Up Proper Standards and Procedures

A well-known global office products manufacturer prudently registered its key trademarked names in many ccTLDs. The company used the ccTLDs to drive traffic to its main .com Web site. However, it failed to utilize a generic, company-controlled administrative contact name and email address.

The employee listed as the domain administrative contact for many of the domain registrations left the company on unfavorable terms. For security reasons, the employee's email address was deleted and he was not allowed access to any company systems. As ccTLD registries continued to send invoices to the employee's email address, the invoices bounced. Because no procedure had been established, invoices sent by mail were not routed properly.

Companies can prevent problems such as this by using a generic name and email address that can be reassigned at the registrant's option at any time. Because the administrative contact for a domain name typically has the authority with most registries to manage almost all aspects of the domain name record, including the Web pages to which the IP addresses point, it is wiser to use an email address such as [admin@company.com](mailto:admin@company.com).

## Top-Level Domains

There are two types of top-level domains (TLDs): generic top-level domains (gTLDs) and country-code top-level domains (ccTLDs). A third proposed type of TLD, sponsored TLDs (sTLDs), is under consideration by ICANN.

### + Generic Top-Level Domains (gTLDs)

Generic top-level domains (gTLDs) are not tied to a territory or country. Besides the familiar .com, .net, and .org gTLDs, lesser-known gTLDs have existed for some time: .edu, limited to North American accredited universities; .mil, reserved for use by the U.S. military; .gov, for the U.S. government; and .int, for use by international governmental and diplomatic organizations such as the United Nations.

The six unrestricted commercial gTLDs are .com, .net, .org, .biz, .info, and .name. Anyone, from anywhere, may register as many available names as desired in any of these domains. (.biz is designated for businesses only, but VeriSign is unaware of any challenges citing this rule, and .name, originally designated solely for individuals, now functions effectively as .com.)

For this reason, gTLDs are sometimes referred to as "unrestricted" or "open" domains.

Global enterprises with valuable trademarks will always place a priority on registering important names and brands in the original and very popular .com, .net, and .org domains. The addition in the past few years of .biz and .info as unrestricted gTLDs, as well as .name, has added to the complexity of the gTLD landscape. Each new domain registry had its own Sunrise and startup registration processes, as well as distinct dispute resolution policies and procedures that supplement ICANN's UDRP.

## NEW gTLDs GAIN POPULARITY OUTSIDE THE UNITED STATES

Because many people outside the United States missed out on the original domain name rush, a much higher percentage of registrations under the *.info* and *.biz* gTLDs are from outside North America. Registrations for these two gTLDs combined have reached 5 percent of overall worldwide registrations as of early 2005.

The biggest growth sector for *.info*, which neared the 3.5 million mark in April 2005, has been in Europe. The continent remains the leading region for registrations, representing 54 percent of total registrations versus North America's 38 percent. Furthermore, as of September 2004, Europe accounted for nearly 70 percent of the dedicated *.info* sites in use, according to Afilias, the registry operator.

Afilias also now offers the capability to register *.info* domain names using the German script umlaut characters ä, ö, and ü. Since the launch of German script IDNs in March 2004, more than 18,000 IDNs have been registered. More than 60 percent of those registering IDN names were brand new customers to the *.info* domain, illustrating the growing popularity of IDNs.<sup>1</sup>

Although *.biz* has enjoyed a fair amount of success in the United States, countries in Western Europe—Great Britain and Germany in particular—have proven to be the most eager adopters of the domain. More than 1 million *.biz* domains have been registered as of April 2005. NeuLevel, the operator of the *.biz* registry, also began offering German-script IDNs in October 2004. According to NeuLevel, Germany is the second largest market for *.biz* registrations.<sup>2</sup>

Although the new gTLDs allowed trademark holders to apply for related domain names on a priority basis during their Sunrise and startup periods, they now allow anyone to register on a first-come, first-served basis.

As of early 2005, more than 36 million *.com* domain names have been registered worldwide, which accounts for 46 percent of all domain names registered, according to VeriSign's March 2005 *Domain Name Industry Brief*.

For *.com*, *.net*, and *.org*, the domain name environment has now reached a steady state. Most of the processes, problems, and solutions are well understood. Effective relief for trademark holders, in the form of the UDRP, has made infringement somewhat manageable. The challenges now are as much internal as external: companies have to be alert and ready to renew their names, periodically review their portfolios for gaps in registration, and remove names that are no longer useful.

Besides the new unrestricted TLDs just discussed, four other TLDs have been introduced in the past few years. All are active:

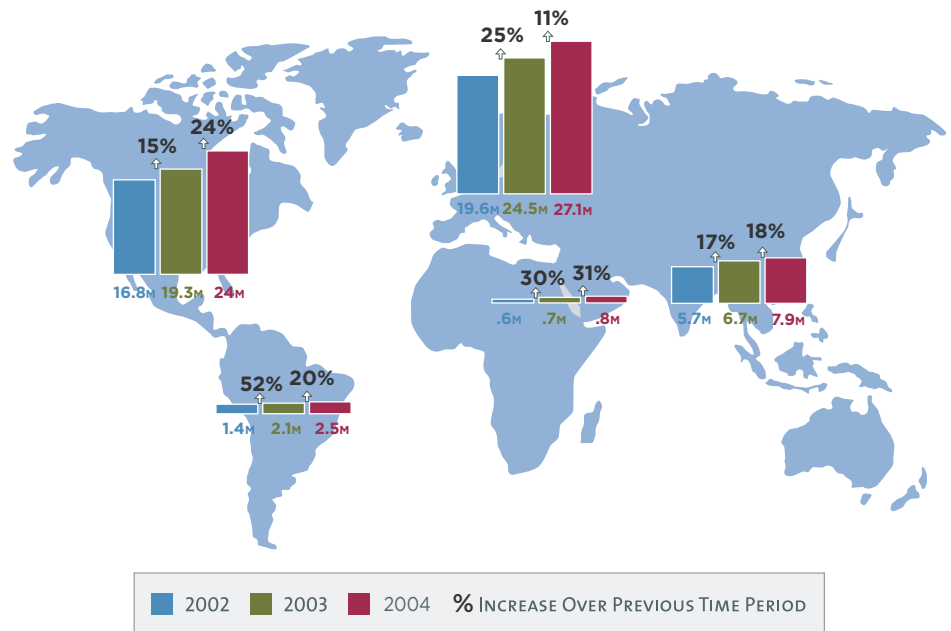
- *.aero*—Restricted and sponsored by the Societe Internationale de Telecommunications Aeronautiques SC (SITA), domain name registrations are limited to accredited aerospace and transport service organizations, including air navigation service providers, aviation media and professionals, suppliers, airports, recreational aviators, and professional pilots.
- *.coop*—This sponsored, restricted domain was established to serve the needs of the international cooperative community. Registrations are limited to accredited business cooperative service organizations. The sponsoring organization is DotCooperation LLC (DCLLC or DotCoop), a U.S. company of which the National Cooperative Business Association (NCBA) is the sole member.
- *.museum*—Sponsored by the Museum Domain Management Association (MuseDoma), *.museum* is a restricted domain. As defined by the International Council of Museums (ICOM), registrations in this domain are limited to museums, museum organizations, and individual members of the museum profession.
- *.pro*—The *.pro* gTLD is an unsponsored, restricted domain that was established to serve the needs of professionals, particularly those in the legal, medical, and accountancy fields. The registry operator is RegistryPro, a subsidiary of Hostway Corporation. Registrations were limited to accredited lawyers, doctors, and accountants for the initial launch in the United States. In 2005, RegistryPro began offering *.pro* registrations to qualified professionals in the United Kingdom, Canada and Germany. RegistryPro began offering *.jur.pro*, *.bar.pro* and *.aca.pro* in addition to *.med.pro*, *.law.pro* and *.cpa.pro* in January 2005. Eligibility will also be extended eventually to the other professions such as pharmacists, educators, veterinarians, and public relation professionals.

In the event of disputes, the UDRP applies to registrations in the above domains, although other dispute resolution processes may also apply. In the case of *.name*, for example, ICANN has adopted an Eligibility Requirements Dispute Resolution Policy in addition to the UDRP.

<sup>1</sup>Source: [www.afilias.com/news/press\\_resources/3yearanalysisSCREEN.pdf](http://www.afilias.com/news/press_resources/3yearanalysisSCREEN.pdf)

<sup>2</sup>Source: [www.neulevel.biz/ids/10.07.04NeuLevelIDNPressRelease.pdf](http://www.neulevel.biz/ids/10.07.04NeuLevelIDNPressRelease.pdf)

### Geographic Composition



Sources: CyberAtlas; Zooknic January 2005; VeriSign January 2005

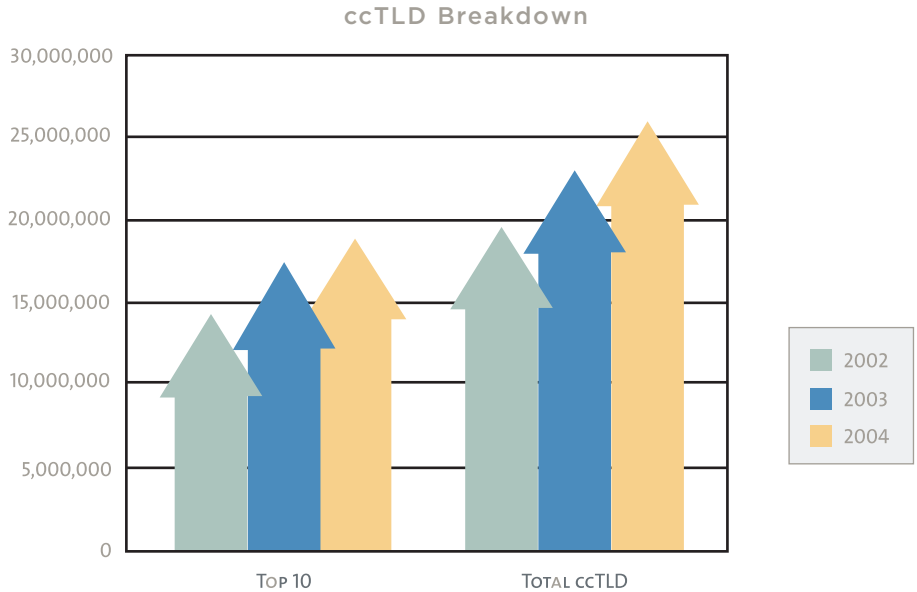
#### + Country-Code Top-Level Domains (ccTLDs)

Although U.S. businesses show a marked preference for *.com* domain names, many international companies place a priority on registering domains in their own country's ccTLD. The *.com* domain may still be the gold standard, but just as Web sites in other languages are gaining ground on English primacy, the importance of *.com* is slowly equalizing in the face of fewer available *.com* names and the rising popularity of ccTLDs.

Many U.S. enterprises have also realized the importance of ccTLDs, even if they don't currently have business operations overseas. In existence for years, ccTLDs have only recently become recognized as an effective means to target and reach consumers in local markets; they now account for 39 percent of all domain name registrations.

A handful of ccTLDs now show marked increases within their specific countries. For example, *.de* represents 90 percent of the total domain name market in Germany. The majority of registrations across all ccTLDs is attributable to a handful of ccTLDs. Of more than 240 ccTLDs, the top ten account for 71 percent of all ccTLD registrations. Total registrations in ccTLDs have surged from less than a million in 1998 to more than 30 million by late 2004, according to data compiled by Zooknic.

As of October 2004, there were approximately 250 primary ccTLDs in which names could be registered. Many ccTLDs also have sub-domains (for instance, *.co.uk*, as well as *.net.uk* and *.me.uk* in the United Kingdom), bringing the total number of ccTLDs and their sub-domains accepting registrations to more than 1,300. The actual number of ccTLDs actively accepting registrations fluctuates based on unpredictable factors such as the creation and/or dissolution of countries, politics, and changes in registry management.



Source: Data provided by Zooknic January 2005

Each ccTLD registry is largely free to register domain names in any manner it sees fit, as in many cases local governments do not control the ccTLD. Instead, most ccTLDs are run by universities, non-profit organizations, and entrepreneurs. As such, each ccTLD often has unique rules and regulations as well as procedures. A review<sup>3</sup> of the 25 countries that comprise the European Union (EU), for example, reveals that many lack a formal dispute policy, and many have not adopted ICANN's dispute resolution policy (UDRP). Several EU registries, especially within the new member states, do not currently offer any type of dispute resolution process, leaving brand owners at the mercy of unclear national laws and local courts where litigation can take months, if not years, and cost thousands of dollars.

Given the uniqueness of each ccTLD registry, it should come as no surprise that renewing these domain names is a painstaking process that requires diligence and, more often than not, relies on relationships with each registry. Some ccTLDs do not send out renewal invoices on a timely or predictable basis, and paying for registrations or renewals in local currency can be complicated. Some ccTLDs, for instance, require that payment be sent by wire and confirmed with a fax or telephone call. Dealing with many ccTLDs requires proficiency in the local customs and language.

Determining what ccTLDs you ought to register depends on a variety of factors. As a rule, if you do business in a country, registering the local ccTLD is usually the proper move. If you do not conduct business in the country, and do not intend to, the local ccTLD would be a lower priority. However, unrestricted ccTLDs should always be considered to be at high-risk for infringement (see the section, Unrestricted Countries).

<sup>3</sup>Source: for more information, see the VeriSign White Paper—*Protecting and Managing Your Company's Online Identity: Domain Names in the Newly Expanded European Union*

As of early 2005, nearly 200 of the 240 ccTLDs were actively registering names. VeriSign classifies these names as follows:

- **Unrestricted**—No local presence is required. Anyone, from anywhere, may register. There is usually no limit on the number of names a company can register. Registration is generally automatic but may take up to a week in some cases.
- **Restricted**—Mild local address presence requirements are imposed, such as local postal address or administrative contact. There is usually no limit on the number of names that can be registered. Registration may take up to two weeks.
- **Severely restricted**—Requirements include the presence of a local business entity, national trademark owner, national citizen, or resident. Registration in these domains may require the registration number of a local business entity or national trademark, a local administrative contact, and extensive proof of the right to a name. It may also require payment in local currency. Registration may take several months.

#### Unrestricted Countries

As of early 2005, an estimated 200 ccTLDs and sub-domains were available in the top 100 unrestricted countries. Anyone from anywhere can register one of these domain names, as in the *.com*, *.net*, and *.org* domains. No local presence is needed. Examples include the ccTLDs for the United Kingdom, Belgium, Mexico, Denmark, Israel, and South Africa. (Note: Specific DNS configuration may be required in some instances.)

Many trademark holders consider unrestricted countries as “high-risk” and rank them as the highest priority for registration. Internet-savvy companies are registering in these country codes in order to protect, extend, and reinforce their brands. They want to be first in Internet markets where the local population may type in local domain name addresses when looking for information or wanting to buy a particular product. These companies seek to cover all possible bases in the quest to maximize traffic to their *.com* and local Web sites.

Many of the unrestricted countries also have sub-domains, posing additional threats to Web identity. For example, in Russia, in addition to the *.ru* domain, there is a *.com.ru* domain. In the United Kingdom, besides *co.uk*, there is *org.uk*. Typically, a business can register one name in all the unrestricted domains for less money than it would cost to litigate one domain name infringement case.

Several ccTLDs have been repurposed as generic domains, including *.cc* and *.tv*. For example, although *.cc* is technically the ccTLD for the Cocos (Keeling) Islands, it is open to anyone, and many companies use it as a primary domain name. Its presence is especially strong in Asia. In the past few years, VeriSign purchased eNIC, the registry and registrar of *.cc* names, and the registry for *.tv*, which was initially created as a result of a business agreement between Idealab, the Internet business incubator, and the country of Tuvalu. The registry is open to all applicants, and registrants have the right to renew indefinitely.

#### Restricted and Severely Restricted Countries

The remaining countries are classified as “restricted” or “severely restricted.” They require a local company and/or specific legal documentation in order to register ccTLD names. Examples include Japan, France, and Canada.

Many companies have franchisees or licensees in restricted countries. As a result, they may be able to register in a restricted country through their associate. This approach may be

## WHAT ABOUT THE EUROPEAN (.eu) DOMAIN?

The European Commission has selected EURid—the European Registry for Internet Domains—as the registry for the .eu top-level domain. The three founding members of EURid manage the country codes .be (Belgium), .it (Italy), and .se (Sweden). The .eu domain will be semi-restricted. This designation means that only organizations established in the EU or private residents of the EU can register names. It is expected that U.S.-based companies with offices in an EU country will be eligible.

Although EURid has signed an agreement with the European Commission, which in cooperation with the EU member states and EURid will determine the rules guiding registrations and disputes, several more steps must be completed before .eu can launch. ICANN has now included .eu in the DNS root servers in order for it to function, and EURid has indicated it will begin accrediting registrars soon. Once .eu registrars are accredited, they will be allowed to accept pre-registrations for their customers.

Depending on how quickly these issues progress, .eu is expected to be operational sometime in late 2005. As with many other new domains, a Sunrise period will allow trademark holders to apply for defensive registrations.

A note of caution: Several companies have been misleadingly offering pre-registration services for .eu domains. Until EURid accredits .eu registrars, pre-registration is not possible, and any company purporting to be affiliated with EURid is in no way connected to the actual .eu registry operator. Additional information can be obtained from the official .eu Web site at [www.eurid.org](http://www.eurid.org) or through VeriSign Digital Brand Management Services.

problematic if the business arrangement with the licensee or franchisee falters, and the licensee or franchisee has all rights to the domain name.

Providing a local address or office may not be enough for the registry authorities. Unless the registry requirements are followed exactly as outlined, it can be difficult to register a name in these countries. However, registration difficulties aside, it is much easier to register first than to try to recover a lost or stolen name, especially when considering the time and money that marketers spend to promote their brands.

As mentioned earlier, many ccTLD registry operators have not adopted ICANN's UDRP. Although ICANN has taken steps to close some of the loopholes in the UDRP, some proactive registries are adopting their own set of standards for dispute resolution, which are often used in lieu of the UDRP.

### + New Proposed Sponsored Top-Level Domain (sTLDs)

New gTLDs have been a long-standing topic of dispute and discussion within the business and technical community. Although the introduction of certain new gTLDs has been generally well-received, as evidenced by their growing registration rates, brand and corporate domain name managers have voiced concerns. This is understandable, given the challenges and costs of properly protecting multiple brands and trademarks in pre-registration periods and recovering names registered by cybersquatters.

These issues are receiving renewed attention as ICANN considers new sponsored gTLD (sTLD) proposals. Along with the adult-content TLD .xxx, other candidates for potential new sTLDs in 2005 include .asia, .cat (for Catalonia), .jobs, .mobi (for the mobile phone industry), .post (for postal services), .tel (for telephone numbers), .travel, and .mail (operators of mail servers).

Although an unsponsored gTLD generally operates under policies established by the overall Internet community working through the ICANN process, a sponsored gTLD, or sTLD, (e.g., .aero or .travel) is supported by a group that represents the interests of a much smaller community and is responsible for managing the implementation and policy issues. Sponsors are generally a consortium of companies and organizations.

As of early 2005, ICANN has given approval for .jobs and .travel. Negotiations will now begin on how the new registries will manage the technical implementation of the domain names. The process could take months however.

As of April 2005, no one has been officially authorized to “pre-register” domain names in the new sTLDs currently under consideration or other potential domain names. Persons attempting to “pre-register” such domain names do so at their own risk and with no assurance that they will receive the pre-registered names if and when the TLDs become operational.

Over the past few years, the U.S. Federal Trade Commission (FTC), the national consumer protection agency, has issued a number of consumer alerts warning of “scam artists” offering domain name pre-registration services, particularly in domains that are not officially recognized or supported by the current root structure. The FTC advises consumers to protect themselves by “[a]voiding any domain name pre-registration service that asks for up-front fees, [or] guarantees particular top-level domain names or preferential treatment in the assignment of new top-level domain names.” Ignore any vendor purporting to offer pre-registration or registration in domain names such as .web, .sex, .global, .usa, and so forth. These domain names do not exist in the current TLD name root

structure and may either not exist at all or require the installation of complicated plug-ins to function properly. See [www.ftc.gov](http://www.ftc.gov) for more information and current alerts. See [www.icann.org/topics/gld-strategy-area.html](http://www.icann.org/topics/gld-strategy-area.html) for more information on implementation plans for the new proposed TLDs.

### + Using ccTLDs to Improve Customer Satisfaction and Drive Revenue

As your company's online presence grows and you expand your global digital brand strategy, one of the most important factors to consider when registering domain names is in which countries you currently do business, and in which countries you plan to do business in the future. Increasingly, local and country-specific search engines and listing services—as well as individual consumers—are practicing the mantra of “think globally, act locally” by giving preference to companies whose Web addresses end with a country-code domain, such as *.jp* for Japan, *.fr* for France, and *.de* for Germany.

Although most U.S. Web users regularly visit Google™ ([www.google.com](http://www.google.com)) and Yahoo!® ([www.yahoo.com](http://www.yahoo.com)) to perform online searches, global businesses should become familiar with localized, or regionalized, search engines and directories. Currently, more than 2,000 search engines cover 216 countries, territories, and regions, from Australia to Zimbabwe. Google has localized versions of its popular search engine for more than 200 languages and countries. For example, you can use [www.google.com.co](http://www.google.com.co) if you are in Colombia, or <http://no.yahoo.com> for the Norwegian version of the Yahoo! Web site.<sup>4</sup>

Another consideration is paid listing services, several of which now manage sites and partnerships in European and Asian markets. These sites allow marketers to write and submit their own site descriptions, and to direct users to sites with country-specific content and domain names. Search results from these companies are also redistributed through partnerships with other sites, so that results are displayed alongside results generated from Web spiders and robots.

You may wish to register brand and product names to enable customers to find you more easily through direct navigation, and as a protective measure against cybersquatters who may try to use your brand or product name in their URL to divert traffic from your sites to theirs. This is of particular concern for many consumer companies whose goods are being counterfeited or otherwise illegally sold online in remote countries.

By localizing your domain names and associated content, you may increase Web site traffic from search engine referrals, and thereby increase sales and revenue by attracting more qualified visitors. You can also improve customer satisfaction and increased revenue by enabling customers to find you quickly and easily in their own language.

## Internationalized Domain Names

IDNs are domain names represented by native-language characters. The native language domain name is followed by *.com* or *.net* (for example, [www.핀테크소아파.com](http://www.핀테크소아파.com)). Registrants must usually meet the same registration criteria that the primary TLD requires.

Not surprisingly, IDNs are very popular with non-English-speaking businesses, and with global companies using the equivalents of their business names in foreign markets. Because non-English speakers now represent nearly 65 percent of Internet users,<sup>5</sup> proactive enterprises

<sup>4</sup>Sources: [www.phillb.com/countrysc.htm](http://www.phillb.com/countrysc.htm) and [www.google.com](http://www.google.com)

<sup>5</sup>Source: Global Reach, Global Internet Statistics by Language, September 2004 <http://global-reach.biz/globstats/index.php3>

are registering IDNs to cover both translations and phonetic equivalents of their brand names. IDNs are an excellent investment from the point of view of protecting intellectual property, as well as enhancing a company's reach into local markets.

For an IDN to resolve, local language characters must be converted into ASCII characters that the Domain Name System (DNS) can understand. 푸른소아과Sign® i-Nav™ plug-in enables people to use IDNs for Web navigation and email, and some Web browsers now have IDN capabilities embedded.

The i-Nav plug-in and more information on additional developments in IDN technology is available at [www.verisign.com/products-services/naming-and-directory-services/naming-services/internationalized-domain-names/index.html](http://www.verisign.com/products-services/naming-and-directory-services/naming-services/internationalized-domain-names/index.html).

## VeriSign Digital Brand Management Services

VeriSign Digital Brand Management Services enables enterprise companies to manage, monitor, and build brand equity in the digital world. Our digital brand experts help Global 2000 companies throughout the United States, Europe, and Asia to consolidate and manage their domain name portfolios, extend brand reach, and build trust in their products and services online.

Global enterprise customers enjoy many benefits and services, including the following:

- **VeriSign® Domain Name Services**—domain name portfolio consolidation and management services, including access to the Digital Brand Manager (a secure, customizable, online domain name portfolio management tool, accessible anytime) and a full range of search, watch, registration, and modification services
- **VeriSign® Global Digital Brand Expansion Services**—assistance in meeting strict domain name registration requirements in highly restricted countries and expanding business globally via localized domain name registration
- **VeriSign® Brand Monitoring Services**—sophisticated data collection, categorization, and filtering tools to monitor brands online and identify new revenue streams
- **VeriSign® Domain Name Recovery Services**—confidential research, negotiation, transaction, and registration services
- **VeriSign® DNS Assurance Services**—complete outsourced solutions to ensure 99.999 percent Web system uptime and performance through VeriSign's primary or secondary DNS management services
- **VeriSign® Consulting Services**—local, in-language consulting in Sweden, Denmark, Norway, France, Germany, and other countries throughout Europe, as well as in the United States

Visit us at [www.Verisign.com](http://www.Verisign.com) for more information.