

Domain Name Management:

Optimizing Brand Protection and Valuation

For corporations with an international presence, the importance of having a comprehensive Domain Name (DN) management strategy cannot be overemphasized. The globalization of business has pushed the marketplace into an international arena driven by the Internet while at the same time placed companies at risk of domain hijacking. Corporations are forced into registering hundreds of DNs to prevent interruption of business and brand dilution by cybersquatters. The damage to a corporation's reputation and the loss of revenue caused by cyber criminals have been documented worldwide.

To determine what actions should be taken to prevent disruption and damage to the company, product or service, a corporation should *thoroughly understand the nature of the threats*. The corporation should then become *informed about best practices in managing Domain Name portfolios* for optimal brand protection and valuation. This should be followed by an *assessment of the current Domain Name portfolio management system benchmarked* against best practices. Finally, a corporation should decide whether it has onboard the necessary *expertise and resources to manage effectively and proactively its DN portfolio*. If not, a corporation should engage the services of a company specializing in DN portfolio protection and management.

THREATS: DAMAGE TO A COMPANY'S REPUTATION AND LOSS OF REVENUE

The Internet Corporation for Assigned Names and Numbers (ICANN) is an international non-profit entity whose mission is to regulate Domain Name registration and monitor domain abuse. The magnitude and severity of the threat to a company is summed up in a 2006 report by the ICANN Security and Stability Advisory Committee (SSAC):

“Domain hijacking can disrupt or severely impact the business and operations of a registrant [company], including ... denial and theft of electronic mail services, unauthorized disclosure of information through phishing web sites and traffic inspection (eavesdropping), and damage to the registrant’s reputation and brand through web site defacement.”

These threats are possible because of vulnerabilities in the DN registration system. The Domain Name System (DNS) works like an automated telephone directory but substitutes the numeric Internet Protocol (IP) addresses with a unique name (usually the brand name). **Registrars** require all prospective Web site **registrants** (DN “owner”) to provide contact information, which is then made available to the public on the Internet through a service called Whois. Each top-level domain or TLD (.com or .uk, for instance) has a **registry** responsible for managing Domain Names and setting policy for the domain. The registrant is responsible for keeping the Whois information current. An expired registration for a DN means it can be bought by a third party with “bad intent,” potentially harming the company or product.

The recent availability of new TLDs has increased the chances of a company's brand name being hijacked by a cybersquatter who (1) acquires a company's Domain Names that have expired and tries to re-sell the names at a high price; (2) registers a company's brand/trademark with a different top-level name taking consumers to a

counterfeit site; and, (3) registers Domain Names identical to a company's DN but with one letter altered (known as typo-squatting).

McAfee, a virus protection software company in the U.S., documented 1.9 million variations of 2,771 of the most popular Domain Names and found that a typical consumer who misspells a popular Internet address has a one in 14 chance of landing at a typo-squatter site (*What's In A Name: The State of Typo-Squatting 2007*). The cybersquatter redirects Internet traffic to the counterfeit Web site, siphoning off business for the company, potentially placing the consumer at risk of identify thief and accessing unauthorized corporate information (US Government Accounting Office 2005 report; ICANN).

The corporate counsel for trademarks for the pharmaceutical company Pfizer said in an interview, "*I think any confusingly similar variant of your brand in a Domain Name is infringement that dilutes your brand and ultimately left unchecked undermines revenue and undermines your brand equity.*" (The Register, August, 2007). Mazerov Research and Consulting (marketing firm in the US) in an independent study found that "*a significant interruption has lasting impact on the company at about 88 minutes. That is, in just under 1.5 hours the company begins to suffer long-term damage.*"

RECENT FINDINGS POINT TO INCREASED RISKS

- at least 8.65% of all Domain Names are registered with false or incomplete Whois information, a practice that makes domain squatting easier (US Government Accounting Office)
- EURid , the Belgium-based registry for .eu Domain Names, suspended more than 74,000 Domain Names and sued 400 registrars for registering the names with a view to re-selling them, in breach of the contract between registrars and the registry (The Register, 2007)
- five non-U.S. countries most likely to have popular sites squatted are the United Kingdom (7.7%), Portugal (6.5%), Spain (5.9%), France (5.4%), and Italy (4.1%) (McAfee Report, 2006)
- cybersquatting disputes filed with the World Intellectual Property Organization (WIPO) increased 48% over 2005

The WIPO noted four recent developments in the DN registration system which have increased threats to businesses large and small:

- automatic registration of expired Domain Names and parking on pay-per-click portal sites;
- option to register names free-of-charge for a five-day tasting period;
- proliferation of new registrars; and,
- availability of new Top Level Domains.

The WIPO believes these developments create increased opportunities for a single third party with malicious intent to register thousands of Domain Names in a short period, infringing on intellectual property rights. And, there has been a tremendous increase in the number of registrars since 2000 which for WIPO *“raises heightened concerns about cases where certain registrars appear to engage in or collude with cybersquatting practices.”*

COMPLICATIONS: ADMINISTRATIVE BURDEN OF MANAGING DN PORTFOLIOS

Monitoring intellectual property infringement and taking preventive measures add to the administrative burden for a corporation. And that does not include the seemingly simple task of updating DN registration to prevent a squatter from taking over a corporation's Domain Names. The recent availability of new top level domains (TLD) is causing corporations to view their Domain Name portfolio in a different light. Just recently (June, 2008), ICANN voted to allow the addition of any TLD that has no more than 64 characters.

Some DN management companies are predicting that multi-national corporations will be registering even more new DNs to stay abreast of the situation. Already corporations have huge portfolios as insurance against cybersquatters. Managing those portfolios has become complicated. According to ICANN, complications arise because of *"the varying circumstances (in terms of type of organization, policies followed, economics, language, culture, legal environment, and relations with governments) of different ccTLDs [country code] and the organizations that operate them."*

LITIGATIONS: PROACTIVE VS. REACTIVE IS THE BEST RETURN ON INVESTMENT

A corporation seeking a legal remedy to the problem of cybersquatting will hit some road blocks. In the US, the Anti-Cybersquatting Consumer Protection Act (ACPA) was passed to protect trademarks owners from abuse by cybersquatters. However, a cybersquatter not based in the US is outside the ACPA jurisdiction.

The WIPO provides a Trademark Domain Name Dispute Resolution Service and ICANN has established a Uniform Domain-Name Dispute-Resolution Policy:

“All registrars in the .biz, .com, .info, .name, .net, and .org top-level domains follow the Uniform Domain-Name Dispute-Resolution Policy (often referred to as the “UDRP”). ... To invoke the policy, a trademark owner should either (a) file a complaint in a court of proper jurisdiction against the domain-name holder (or where appropriate an in-rem action concerning the Domain Name) or (b) in cases of abusive registration submit a complaint to an approved dispute-resolution service provider.”

The upshot is that apprehending the cyber criminal is costly (legal fees), time-consuming and seeking damages for lost revenue is often unproductive. Resources should be devoted to preventive measures rather than to litigations. The fact is, corporations, especially the banking, retail, and pharmaceutical industries, are constant targets of cybersquatters operating globally. An individual in China, who recently registered 10,000 Domain Names, drew suspicion by a European registry. The registry suspended the individual's domain registrations, questioning the need for a single person to have so many Domain Names. Without a proactive management strategy, corporations with huge DN portfolios could find themselves bogged down in frequent and ongoing litigations.

A proactive strategy, then, is to cut the cybersquatters off at the pass by having in place an effective and comprehensive DN portfolio system. But, the ROI (return on investment) for a corporation's portfolio entails much more than management. The DN is a marketing tool and adds value to your trademark/brand. Furthermore, there is a clear advantage to registering local domain names. Search engines like Google tend to rank the Web site based on the TLD origin. For instance, a .fr Web site in French will be more visible in France than a .com in English. That is because potential consumers surfing the Internet purposely filter results to obtain local results.

SEVEN BEST PRACTICES FOR DOMAIN NAME PORTFOLIO
MANAGEMENT

View Your Domain Names as a Corporate Asset

Is the management of your Domain Name portfolio an integral part of your total business management strategy? Is domain portfolio management in sync with your corporate objectives and goals? If the answers are no, this is your first clue that your company has failed to see your DN portfolio as a valuable corporate asset to be protected and valorized. The risks are too great not to have a comprehensive domain management strategy. And, the opportunities to valorize this asset are too numerous to be ignored.

Centralize Domain Name Management

Choose a single, accredited registrar for your DNs to reduce costs and risks and have a single-point of contact (corporate administrative contact). As new top level domains become available and as the corporation builds its e-commerce for products and services, the necessity of continuously acquiring new Domain Names can result in too many opportunities to miss renewal deadlines. You should not only have an effective management system but a comprehensive strategy to protect and optimize your brands and trademarks.

Perform Systematic DN Portfolio Audits

Audit all your Domain Names immediately. Do managers in different areas of the company who control Domain Names have the same policies for renewals and management? After an enterprise-wise audit is performed, you should develop policies and procedures for systematic renewals and acquisition of new domains.

Audit and Centralize Your Trademark Portfolio at the Same Time

Many countries require a new trademark or a local company to also register a domain name. This is true for France. So, audit and centralize your trademark portfolio at the same time you centralize your DN portfolio.

Monitor Domain Registration Information for Guaranteed Renewals

Take steps to ensure you have the resources and technology for guaranteed domain renewals and control over the process. Failure to update Whois can result in losing DNS to cybersquatters who will try to resell the DNS to you at exorbitant prices or redirect Internet traffic to a bogus or counterfeit Web site. Renewing your DNS for periods longer than the usual two years will ease the administrative burden. However, with large portfolios, having different initial registration dates for DNS, managing renewals can be an administrative hassle leading to mismanagement of this valuable asset.

Stay Informed About New Threats

Do not wait until the crisis (the counterfeiting, the disruption of services, or unauthorized access to company and consumer information) occurs to take action. Devote resources to monitoring the threats on the horizon, assessing the potential harm, developing a plan and taking action to protect your DN portfolio asset.

Monetize Domain Names

The commercial and marketing use of domain names is a key element for brand valuation; a well managed domain name portfolio can reduce the advertising costs by several thousand Euros. This can largely compensate the expenses of new domain names and the domain name management expenditures.

OUTSOURCE DOMAIN PORTFOLIO MANAGEMENT FOR OPTIMAL
BRAND PROTECTION AND VALUATION

VAYTON has the expertise and cutting-edge technology for managing your Domain Name (DN) portfolio and optimizing brand protection and valuation.

Expertise: Outsourcing DN portfolio management to VAYTON may be the wise choice for your company. A dedicated team of experts can ease the burden of DN portfolio management at all levels: administrative, technical and strategic.

Comprehensive Services: You can count on a comprehensive suite of services necessary to prevent brand devaluation and security compromises. VAYTON will audit, monitor, centralize, renew and recover your domain names.

Cutting-Edge Technology: VAYTON has developed technologies and platforms to audit, monitor and centralize domain names. These technologies are customized to answer decision makers' as well as technical team requirements.