

A domain name policy in 10 easy steps

Gretchen Olive provides a list of stages that every brand owner should consider when drawing up a corporate domain name policy

Over the years, companies have gone to great lengths to meticulously create and administer trade mark programmes that identify the circumstances in which a brand is trade marked, how it should be monitored and the mechanisms that should be employed for enforcement. However, to date many companies have not been as disciplined and have not dedicated comparable time and resources to defining a domain name policy. But why?

Some suggest that the challenge lies in the fact that the registration and management of domain names within an organization is often a shared responsibility across several departments – legal, marketing and IT. Without a single champion and budget line dedicated to the cause, the creation of a comprehensive domain name policy quickly gets relegated to the “nice to have” category, as opposed to being viewed as a “have to have” due to the difficulty in securing consensus, budget and staff resources across multiple departments for such an effort. In sum, everyone has a day job and there is little time, money and energy left to be a Good Samaritan without a mandate from the highest levels of management to get a domain name policy on the books.

The problem with this approach is that the internet is growing in size and consumer influence faster than any other channel. With more than 153 million domain names registered worldwide (an increase of more than 33 million from 2006), the estimated number of internet users reaching 1.4 billion and growing each day and recent surveys confirming that consumers rely on the internet as their primary source for news and information, it is more critical than ever for companies to transcend these departmental boundaries and constraints and develop a comprehensive domain name policy to secure, promote and protect their brands online. Failure of brand owners to do so sooner, as opposed to later, will not only result in impairment to the health of their corporate brands, but also negatively impact their bottom-line in this global economy.

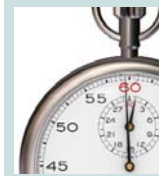
Mapping out an effective domain policy

An effective domain policy is one that outlines the specific goals and objectives of an organization, clearly defines individual stakeholder/department roles and responsibilities, creates sustainable and enforceable policies and procedures to deal with everything from registration to recovery of domain name assets, and can adapt to changing conditions. While this may sound like an overwhelming endeavour, by following the 10-step approach below, your company can be well on its way to reducing risk and cost and leveraging the internet to grow its business and brands.

Step one: define goals

The late Peter Drucker, often referred to as the “father of modern management” once said: “Objectives are not fate; they are direction. They are not commands; they are commitments. They do not determine the future; they are means to mobilize the resources and energies of the business for the making of the future.” In devising your company’s domain name policy, perhaps no other step is more critical to the policy’s future success than a clear definition of goals. Before putting pen to paper, sit down with all the stakeholders in your organization and understand their strategic business goals, understand where they have experienced pain in domain and brand administration in the past, have them talk about domain name initiatives and procedures that have worked well and ask what they think the top three objectives for the company’s domain name policy should be. It is important that this is a very candid discussion, where titles and feelings are left at the door, and participants not only come from management ranks, but also include those from the trenches.

One-minute read



Most companies do not have a written domain name policy. This often leaves staff, management and contracted third partners in the dark as to the who, what, when, how and why of domain name management within an organization. But today more than ever it is critical for companies to transcend departmental boundaries and constraints and develop a comprehensive policy to secure, promote and protect their brands online. A domain name policy development process will add discipline, visibility and accountability to the promotion and protection of your corporate identity and brands online. This 10-step process covers goals, responsibilities and overall strategy as well as day-to-day operations, budget, reporting and review. It should improve the health of your brands and benefit the bottom-line.

There is no set formula for the right number of goals, but it is important that they are specific and measurable. For example, reduce the number and cost of domain name recovery efforts by 10% or enable all business units to have online access to the portfolio of domain names and related data attributable to their business. In addition, it is imperative to develop goals that represent the consensus of the stakeholders. Consensus, while sometimes difficult to achieve, will enable you to depend on champions of the cause throughout the organization and create an environment where all interested departments have a vested interest in a successful domain policy implementation.

Step two: assign roles and responsibilities

At the heart of any good policy is a clear understanding of roles and responsibilities. Stakeholders must quickly answer

There will be a temptation to dive into all the "tasks" that are involved in managing a domain name portfolio. Resist

several fundamental questions: will the company outsource day-to-day management of domain assets or will internal staff be responsible or will a hybrid approach be taken?; will there be a central domain name administrator who will manage the portfolio or will each business unit be responsible for managing its own portfolio?; which department will bear primary responsibility for administration, what checkpoints and controls are necessary to prevent allegations of infringement by outside third parties and who will ensure the security of company domain and website assets? Once you have answered these baseline questions, make a list of high-level responsibilities for various components of your company's domain name policy and map them to departments/individuals/vendors. There will be a temptation to dive into all the "tasks" that are involved in managing a domain name portfolio. Resist. All you want to achieve now is a list of the players/stakeholders and their high-level responsibilities within the policy. Think of it as your domain name policy organizational chart. Don't forget to consider the role subsidiaries, franchisees and other business partners may need to play.

Through this process you should also designate a leader – someone who will sit at the top of the domain name policy organizational chart. This leader is not necessarily the person with final say and ultimate responsibility for all domain name decisions, but this person should at least be viewed as the primary facilitator and the authoritative source for domain name policy questions.

Step three: determine strategy

With your goals and objectives in hand and the high-level areas of responsibility mapped out, it is now time to talk strategy. Ask what is your organization trying to achieve on the web? Is it brand protection, brand promotion/awareness, revenue generation, information distribution, or all or some combination of the above? If you have more than one objective, what is the order of priority and how much risk or cost can you incur to support each? Which markets are you operating or trade marked in? Which markets does your company expect to be operating in the next one, three or five years? What extensions present the highest level of risk to your business?

If brand protection is an objective, compare your existing

domain name portfolio to your trade mark portfolio and list of company names to determine meaningful gaps, identify infringements and pinpoint defensive registration opportunities and potential domain names to let lapse. If brand promotion/awareness, revenue generation and/or information distribution are your objectives, understand how internet users are searching for you and your brands on the web by conducting a keyword analysis. With direct navigation on the rise, it is more important than ever to have both a keyword/search engine optimization strategy and a domain name registration strategy that work together.

Discuss how the company should determine which extensions and brand strings to register for new TLD launches, new brand launches and other important business events. Recognizing that budgets and resources are limited, this is where you need to seek empirical data and assistance from a

trusted adviser who has the experience, data and tools to conduct a thorough analysis and help you make strategic determinations. Do not do this analysis alone; it will be a long and frustrating process to gather the data manually. Data gathering tools and advice are available and can eliminate hundreds of

staff hours spent manually compiling data.

Step four: outline day-to-day mechanics

This step outlines the mechanics of the day-to-day implementation of your domain name strategy. Minding the details during this step is perhaps where the biggest administrative cost reductions and mitigation of risk can be realized. Be sure to consider the bigger picture – where and when should domain name registration fit into the company's branding policies, creation of new business entities or other important business events, like a merger and acquisition?

Flow chart how availability searches and domain name requests for registration, renewal, transfer and modification should be handled not only by those within your organization, but also by outside third parties/consultants who are helping the organization screen, search and register trade marks, create new business entities, build websites, develop online strategies and close new business deals. It is strongly recommended that you develop procedures that require strategic domain name registration simultaneous to any public filing or expression of intent to apply for a name or brand. Reports of domain name front-running where Whois search query data or additions/changes to public database records have resulted in opportunistic domain name registration by third parties have been well-publicized since the start of the year. Because policy always lags behind technology, position your organization to be proactive so you can eliminate the costs associated with domain name recovery of these names down the road.

Also consider what controls and documentation requirements you want to have in place to ensure your actions do not infringe on the ownership or trade mark rights of others. Document what information, approvals and/or forms that are required to process a registration or transfer of domain names (such as purchase agreement, registrant name change agreements or trade mark assignment), make a DNS change or renew a domain name.

Step five: monitoring, escalation and enforcement mechanisms

A recent analysis of more than 100,000 domain names that we carried out revealed that three out of every four domain names

containing a brand are not registered by the brand owner. Furthermore, 34% of the brand-related sites held by third parties used their domain names to operate pay-per-click (ppc) sites. These statistics not only highlight the pervasiveness of brand abuse in domain name registrations, but also provide insight into the potential negative impact on online traffic and in the end, revenue, for brand holders.

In developing your monitoring programme, identify key brands that should be monitored and define the type of infringements that matter most to your organization (for example, hate sites, traffic diversion, sale of counterfeit goods). Ad hoc, manual monitoring is an option, but it is not recommended. Survey monitoring tools and services that are available in the market. Do not accept monthly monitoring reports that are nothing more than data dumps: demand prioritized and categorized results that are actionable and can be reviewed quickly.

The definitions of the various forms of infringement you develop will serve as the foundation for your written escalation and enforcement policies and procedures. Catalogue each potential type of infringement, define the escalation points of contact and the suggested enforcement mechanisms (such as continued monitoring, issuance of a cease and desist letter, DRP, court action and/or site takedown) that would be appropriate based on urgency, cost and risk of harm to consumers and the reputation of the company. This will take the guesswork out of who to turn to and what needs to be done to report problems, minimize liability exposure and preserve evidence in times of crisis.

Step six: identify budget

In order to enable your domain name policy to be more than words on a page, the stakeholders should determine how each aspect of the domain name policy – registration through monitoring to enforcement – will be funded. Sometimes it will be necessary to pool funding from various subsidiaries or departments to fund parts of your policy, such as to fund monitoring tools. The key to success in these situations is to gather functional requirements from all budget contributors and find a solution that can be customized without additional expense. In instances where you must seek additional corporate budget to fund initiatives, use your domain name policy as a tool to demonstrate the careful consideration and justification for your request.

Step seven: create standards

To ensure scalability, transferability and sustainability of your domain name policy, it is critical to standardize communications, data and resources wherever and whenever possible. Start with defining Whois templates that should be used for all domain names owned by the company and its various business units to ensure no individual has the ability to hijack or hold company domain names hostage upon termination of their employment. Create and publicize distribution lists where requests can be sent and notices can be directed from your registrar, registries, DRP agencies and

10 steps to an effective domain name policy

- 1 Define goals
- 2 Assign roles and responsibilities
- 3 Determine strategy
- 4 Outline availability search, registration, renewal, transfer, modification processes and procedures
- 5 Establish monitoring, escalation & enforcement mechanisms
- 6 Identify budget
- 7 Create standards
- 8 Set DNS controls
- 9 Define reporting
- 10 Create a policy and compliance review process

other vendors. This ensures there is no single point of failure in the communication chain. Lastly, create a central repository where specialized tools and resources (such as Whois look-ups, global availability searches, request templates, traceroutes, domain name forms and a copy of your domain name policy) can be accessed by all internal and external stakeholders to ensure consistent handling of domain name matters and to safeguard the security and confidentiality of your activities.

Step eight: set DNS controls

It is estimated that 29% of website downtime is attributable to DNS failure which can create a loss of more than \$1 million a year per organization. Thus, it is important to outline DNS controls to minimize the potential of an outage. Define the type of names (such as live sites, e-mail, redirects) that should be on globally dis-

persed DNS, either hosted internally or through a third party, as well the types of names that can reside on less redundant DNS. Determine if DNS slaving is something your organization wants to implement and set out how and with whom that should be set up. Finally, clearly define the circumstances, personnel, procedures and authorizations that your organization will require to make changes or modifications to DNS.

Step nine: define reporting

To ensure expectations are clear and communication among stakeholders is effective, your domain name policy should also define the type and frequency of reporting that will be available to various parties within the organization, as well as whose responsibility it is to generate each report. This will enable people to understand the type of information they will be receiving on a regular basis (such as quarterly portfolio reports to help review of upcoming expirations to determine renewals and lapses), how progress will be tracked and what information can be pulled from the database when conducting corrective action reviews.

Step 10: policy and compliance review process

It is important to pre-set periodic reviews of the domain name policy, its effectiveness and an evaluation of organizational compliance. This is an important mechanism for stakeholders to determine if the policy is working as intended and where it can improve. It also provides a forum for discussion of new policy provisions to deal with situations not previously contemplated and to assess whether the policy has strong enough teeth to adequately prompt compliance.

By considering and utilizing these 10 steps in the development of your domain name policy you will find yourself wondering how your organization ever did without it.



Gretchen M Olive

© Gretchen M Olive 2008. The author is director of education and industry affairs at Corporation Service Company