Online Brand Protection: A Step-by-Step Guide to Creating a Proactive Strategy

Abstract

As the Web continues to become a more dynamic and vital part of every corporation, today’s enterprises need to become more proactive at anticipating exploits and abuses that can tarnish their reputation and negatively impact their business operations by consolidating their Internet domain names and putting in place a series of protective measures. This paper shows you the steps you need to take to monitor your total online presence and strategically protect your various corporate brands, trademarks, and domains.
Contents

Introduction ............................................................................................................ 3
Steps to Take ......................................................................................................... 4
  Identify All Domain Names in Your Portfolio ............................................. 4
  Manage Your Portfolio Proactively ......................................................... 5
  Monitor for Potential Abuse ................................................................. 6
  Respond to Abuse ................................................................................ 8
Summary .......................................................................................................... 9
Introduction

The Internet has made it possible for companies to quickly expand their ability to do business across many different countries, cultures, and continents, and with relative ease that even just a few years ago was unheard of. But the same technologies and techniques that make it easy for corporations to have this global reach are also available to criminals, who are getting smarter at figuring out ways to abuse brands for their own profit and do so by hiding behind the anonymity of the Internet. These abuses cover a wide range of activities, including infringing pay-per-click sites, false association, automated phishing expeditions and cybersquatted domain names. The latter continues to be the most popular exploit and because the most common dictionary words are already used for domains, domainers are increasingly turning to brand names and trademarks when they register infringing domains. In fact, according to the MarkMonitor Brandjacking Index™, cybersquatting increased by 33% last year.

In addition, cybersquatters continually take advantage of the Internet and the system to evolve their abuse tactics. For instance, domain abusers that continually reserve, test out a domain name, release it at the end of the five-day ICANN grace period, and then re-register the domain name are called Domain Kiters. These abusers don’t have to pay for owning the domain, they can place banner ads to gather even more money and “test market” the kited domain to see what name produces the most revenue. The resulting infringing pay-per-clicks can add up to significant lost revenue for the legitimate brand owner as they’re unknowingly paying for click-thrus coming from these sites via advertising intermediaries. In addition, these sites can create real consumer frustration, ultimately resulting in a loss of trust and confidence in the brand. While ICANN is evaluating a number of solutions to this problem, some may be more effective than others in dissuading domain kiters.

These threats hurt sales, reduce overall consumer trust, and dilute the brand equity that your company has carefully built over the years, and do so in a few days or weeks with some well-timed attacks. This is why online brand protection has become so important, and why it is another current-day essential business concern. Even The Wall St. Journal has recognized this trend: “Protect your reputation. Your good name is your most vital credential and once damaged can’t be easily repaired—even if your business prospers and you devote yourself to good works.” (August 27, 2007)

In the past, companies have tried to protect their brands through manual methods, such as the occasional search engine query or by setting up a few Google Alerts on their key brands. However, this approach doesn’t work as the Internet is constantly evolving, domain attacks happen almost continuously, and as a result, infringing sites and Whois records often change before the brand owner has a chance to take action. In addition, the dynamic nature of
the Internet makes it difficult to collect and store evidentiary data for possible future action.

The ideal online brand protection program should be a coordinated, cross-departmental and automated approach that goes beyond just the legal department and involves brand management, marketing, loss prevention, risk and supply chain management. This protection also needs to be more proactive, where you track down abusers before they become repeat offenders, and head off any potential problems with reputation, brand confusion, or diverted site traffic and its associated click stream and revenue.

Steps to Take

The ideal online brand protection strategy consists of both technological and organizational programs that encompass the following four steps:

- Identify all domain names in your portfolio
- Manage your portfolio proactively
- Monitor for potential abuse
- Respond to abuse

Let’s discuss these in more detail.

Identify All Domain Names in Your Portfolio

Because domain names are key to the creation of intellectual property assets that establish and secure brand presence on the Internet, the first step is for you to take a careful inventory of all your domains: knowing which registrars are used for which domains, when they are set to expire, and who within the corporation was initially responsible for registering the domains involved. Often, your corporate domain name portfolio grows organically and slowly, with multiple purchasers from across the corporation acting independently to acquire new domains.

Taking an inventory of all domain names can be a daunting task, especially for the typical large multi-national corporation. As an extreme example, one global financial services firm has 5,500 registered trademarks, 2,100 domain names and 2,480 active company names. Even smaller organizations often have more domain names than they think, especially when the scope is expanded beyond core brands and products to include slogans, campaigns and other assets relevant to a company’s business.

Part of the inventory process should include understanding why certain domains were registered in the first place; a review of your existing policies and corporate branding objectives; and ensuring that there aren’t any gaps in your existing domain
portfolio. You’ll want to make sure that your domain policies are in line with your overall business objectives and are consistently applied across subsidiaries. Some of these objectives may include:

- Promoting your brands effectively via the Internet
- Protecting all of your intellectual property assets online
- Extending your online presence to all countries that you do business in
- Being sensitive to the various cultures and nations that you do business in with the right series of international domains
- Managing your domain registration and renewals process cost-effectively

Based on this analysis, you can begin to see what changes you need to make to your domain portfolio in order to ensure that your assets are protected online and you have sufficient coverage in all relevant geographies.

Manage Your Portfolio Proactively

The keystone of any effective domain management program is visibility and control. The answer for most large global corporations is to centralize and coordinate all domain registration with a single corporate focused registrar — consolidation. With consolidation, corporations can begin to proactively manage their domain names and create their ideal domain portfolio by either acquiring or divesting themselves of domains to match their strategic goals.

Ideally, a centralized domain policy should reduce errors, automate domain renewals to prevent domain registrations from inadvertently lapsing, and cut down on duplicated efforts from within your company. A centralized, consolidated domain policy can also help you become more proactive in establishing and protecting your brand online — by giving more visibility into the process of acquiring domain names.

Once you consolidate and have complete visibility into your portfolio, you can begin filling in the gaps with offensive and defensive domain registrations. Offensive domain registrations ensure that you own domains in countries where you’re currently doing business or intend to do business. While defensive domain registration entails registering names that your company does not intend to use, but could potentially be abused by cyber criminals. By registering defensive names — such as “suck” sites or domains containing common misspellings of key brands or trademarks — you can prevent cyber criminals from exploiting domain names associated with your brand. Both approaches are necessary to achieve proactive brand protection.

In addition to offensive and defensive domain registrations, you may periodically need to strategically acquire domain names anonymously for certain purposes — such as
during a product launch, merger or acquisition—or, you may need to acquire about-to-expire domain names owned by third parties, a practice called domain snapping. Bottom line, corporations need to continuously assess, modify and manage their domain portfolio to reflect changes in their business and the evolving risks on the Internet.

### Monitor for Potential Abuse

Creating an ideal domain portfolio is a good start to establishing and protecting your corporate brands online. However, it is just the beginning. While defensive registrations enable you to own and control the domain names that may be abused by third parties, it is simply impossible for any corporation to register every potentially harmful domain name. Therefore, the next critical step for defending your brands online is to establish a strategic monitoring program that constantly searches the Internet for potential abuses, including:

- Cybersquatting
- Domain kiting/tasting
- Trademark infringement
- Traffic diversion schemes
- False associations with unrelated third parties
- Pay-per-click abuse
- Sponsored link abuse
- Logo/image abuse
- Offensive content
- Channel non-compliance with brand guidelines and/or pricing

As part of the process of creating a monitoring program, there needs to be a central brand integrity role created whose job it is to identify the key stakeholders within the company who can recommend registrations, evaluate suspicious sites, respond to potential abuses, and put automated monitoring programs in place. Because of the technological nature of the Internet and the fact that automated hacking tools are being used by the abusers, technology is really the only way to fight back. Ideally, these automated brand abuse monitoring tools should keep track of how your key brands are used on the Internet. This could include the following:

- Combing through millions of websites, domain registrations, blogs, message boards, paid search links daily
- Automatically identifying where potential brand abuse is occurring in page title, meta tags, visible text as well as hidden text
- Quickly and easily investigating the domain/website owner and determine if he/she owns other potentially infringing websites
- Automatically capturing evidence so that the brand owner has records on why they took action, in case the site is taken down
- Tracking case resolution and responses
- Sending automated enforcements

Another part of setting up a coordinated monitoring program is to determine what level of response is needed and how to justify the resources to be dedicated to an effective program. Because it isn’t feasible to review all potential Internet sources of abuse, you should develop your own set of common criteria for judging and prioritizing the various observed abuses. For example, various stakeholders within your company may place different emphasis on things such as offensive content, whether it is more important to stop eCommerce sites selling your goods, offenses by authorized partners or third-parties, whether significant traffic is diverted via the site, and whether the brand name appears in the domain vs. content of the site. Setting up a common criteria guide in addressing online abuse for your company, will ensure that a uniform approach is executed, according to company strategy.

Corporate brand managers should assess the degree to which website traffic is diverted to sites that abuse its brand and the amount of lost advertising revenue that is diverted to fraudulent pay-per-click sites. You should look at both quantitative and qualitative indicators, including:

- Degree of fewer “negative impressions” due to successfully shutting down websites which degrade your brand
- Improvement in website traffic due to successfully shutting down traffic diversion tactics (i.e., cybersquatting, pay-per-click sites, paid search ads)
- Better quality response rate to online advertising due to successfully shutting down fraudulent pay-per-click sites
- Productivity gains and/or hours saved per week in detecting and responding to infringement by leveraging available technologies and solutions

From this information, you can calculate the return on your investment from your online brand protection program and further focus your efforts at the largest paybacks.
Respond to Abuse

Many different responses are possible when an exploit is discovered, and part of any effective program is an understanding of how to match the appropriate level of your response to the particular infringement. For example, there are simple warning letters to the infringing domain/website owner that can be the least threatening but sometimes accomplish your goal. Some more formal measures include cease-and-desist letters to the infringing domain/website owner, a takedown notice to the domain’s Internet provider or, in the case of paid search abuse, a policy violation notice to the search engine. There is also the Uniform Domain-Name Resolution Policy (UDRP) process to reclaim the abused domain, which can be the most time-consuming and expensive, but also the most effective: according to the World Intellectual Property Organization (WIPO), 85% of their panel decisions are resolved in favor of the legitimate brand owner. Finally, trademark litigation can be commenced as a last resort against the most egregious offenders of your company’s brands.

In order to determine which forms of abuse you should focus your enforcement efforts against, you should first examine what the expected business benefit will be, in terms of revenues, customer satisfaction or trust, or other metrics, from combating the abuse. Next, you should examine the type of exploit, whether it is pay-per-click fraud, an attempt at diverting traffic, a squatted domain or unauthorized use of your logos or trademarks — and the degree of threat that the particular category of abuse poses toward your brand. Next, you should try to quantify how much traffic is involved in each abuse and whether a single entity owns multiple infringing sites. Finally, you need to match the response to the expected benefit, and focus on the sites with the highest traffic or the most flagrant abuses first.

Summary

Implementing a comprehensive domain strategy and being vigilant about how your brands are represented online is paramount. Many brandholders have been successful in defending their brands, including high profile legal cases from Dell, Verizon, and Microsoft. This has begun to send a message to brand abusers that they run the risk of litigation and will end up paying for punitive damages. In the cutting edge case of Dell v. Belgium Domains filed in October 2007, Dell sued several of the larger “domain tasting” registrars, using the novel application of counterfeiting laws to protect its famous brands against continued attacks by these cybersquatters.

Future online brand abuse is a near certainty for just about every current business. The Internet is only becoming more complex and dynamic, and as such is a great place for criminals to operate. With new blocks of domains coming available and the increasingly international scope of many businesses, a brand abuser has an
exponential number of potential targets. Plus, the low cost and plentiful availability of hacking tools makes it easy for them to continue to operate. Protecting your brand with manual, ad hoc methods is no longer prudent or effective. A company needs to set up a solid domain name protection strategy, taking a more holistic and technologic approach to control their brands and protect their intellectual property. These technologic means are really the best course, and can pay huge dividends by being proactive — it is less time and resource consuming to address abuse before it occurs, than to rectify the effects of an online attack after the fact. Many companies have been able to trim costs and reduce their exposure to potential fraud with their numerous brands. You can too!
About MarkMonitor

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

To learn more about successful domain portfolio management and other online brand solutions and services, please visit www.markmonitor.com/products

More than half the Fortune 100 trust MarkMonitor to protect their brands online.

See what we can do for you.

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