A Complete Guide to Corporate Domain Portfolio Management

WWW.NETWORKSOLUTIONS.COM

Where to Begin?

Domains names are at the heart of every business's web presence. They define how companies are recognized online and reinforce their identities in a memorable way. Domains serve as anchors for virtual storefronts, billboards for brands and indicators of trusted resources. Protecting intellectual property, supporting new service and product launches and boosting marketing campaigns are just a few of the many uses businesses of all sizes find for domains. U.S. eCommerce grew by 44% in 2020, [1] which serves as both an indicator of how web presence is increasingly more important than physical presence and of just how much domain names matter. The problem, as anyone who has ever been in charge of a domain portfolio can attest, is managing those names.

Unsurprisingly, businesses such as Coca-Cola [2] and Unilever [3] and other large organizations [4] are reported to own thousands of domains. But smaller organizations often have sizable domain portfolios that require serious care and attention. When managing a domain portfolio, there are many technical considerations to ponder, such as understanding and using the Domain Name System (DNS), deciding who oversees the portfolio and which stakeholders will undertake which duties. There are also financial impacts to consider, and matters of corporate reputation at play, which make proper monitoring and maintenance of your portfolio essential.

But where do you begin when it comes to corporate domain portfolio management? As the complications pile up, and further complexities — such as how the domain names intersect and interact with your existing brand names and corporate trademarks — develop, how do you get and keep a handle on everything?

It all starts with a plan.

Table of Contents

Chapter 1

Defining Your Corporate Domain Strategy

You should think of your domain portfolio as a living, breathing corporate entity. It should evolve with the times, adapting as the Internet namespace grows and changes. On a basic level, your strategy should address the following:

- How and when to purchase specific names and when to renew them or not renew them.
- How to protect your existing and future name portfolio.
- How your portfolio relates to your trademarks and how you coordinate them.
- How you safely retire domains that no longer align with your business needs and strategy.

The first step is to complete a **thorough domain asset review and inventory**. Before you can do so, you'll need to determine who is responsible for purchasing new domain names throughout your organization. One of the biggest issues when it comes to domain name management is the fact that a domains affect many different corporate stakeholders. Your marketing department could be working on a campaign that requires a new domain name to correspond with a brand, product or promotion. Your legal department may need a domain to match an existing or anticipated trademark. And your IT team will have networks and servers that need to respond to the name servers that will ultimately be put in place.

Getting these three perspectives aligned and sharing in the decision-making process isn't easy, because it often involves assembling a team of people who aren't used to working together. Without a strong alignment, certain elements may fall between the cracks, creating redundancy, or worse, critical oversights with serious implications. Too many people getting involved often lends to assumptions that others will handle specifics that could get overlooked entirely.

If a corporation's trademark and domain name portfolios aren't managed by the same department, there also needs to be coordination between departments for consistency. This means you need to find all corporate entities that have previously registered domains, as well as those subsidiaries that have been acquired or sold over the years.

You may uncover domains that a subsidiary purchased, as an example. As part of your inventory, make a note of when the domains are up for renewal and which registrars were used.

Second, you should **determine what your overall corporate objectives** for your domain name collection will be and how far from these objectives you currently are. If your company is an online retailer, you might want to have your names match your key product lines and brand names, particular geographic areas where your products are sold or registered trademarks. That last approach is complicated by the fact that the overall domain name space is more dynamic than the trademark space. Additionally, there is no central registry for domain names as there is for trademarks, and, since a trademark does not guarantee you a matching domain name, you'll need to keep careful track of domain availability. Bear in mind that not all trademark disputes resolve in favor of trademark holders, especially when it comes to newer domain extensions. According to the World Intellectual Property Organization (WIPO), [5] cybersquatting cases are on the rise, so understanding which of your preferred domains and extensions are available, and promptly securing those that are, is essential.

Another key choice to make is deciding **whether you will mostly be protecting your brands or promoting them**. An example of a protection plan is purchasing popular "legacy" top-level domains (TLDs) such as .com, .net and .biz, to start with, along with "abuse" domain extensions such as .sex and .sucks, plus any common misspellings of your domain name. For example, if you mistype "googel.com" you will be brought to the correct Google search page because the company purchased this similar name. A promotion-based plan would encompass a larger domain name collection and involve registering multiple spelling variations, creative spellings and abbreviations, shortened versions of your brand name (including creative conjugations), TLDs and country code domains.

Next, **craft your enterprise-wide policies**. These should include who is responsible for registering new domains, who can modify the domain details and other settings and the specifics on what contact information will be included with each name. This latter element is critical, because if emails are being sent to a contact that is no longer an employee you may miss critical renewal messages or other correspondence from your registrar. A better choice would be to create and monitor a group email box such as admin@company.com. This can be used to send messages to a small group that is always available to respond to these requests.

Another set of policies might involve specifying which servers your domains point to. Should your names resolve to your main corporate website, a specific subsidiary or departmental websites? What about the name resolution for country-specific domains that are written in that country's language? Should your websites have standard points of contact for public relations and press, support, investor relations and other departments clearly indicated as well? What about renewal timing? What are the implications for your budget and profit and loss statements? What renewal options does your vendor provide? Will you incur costs earlier with early renewals via settings like auto-renew, save money in the long run by locking in discounts or risk losing domains if you renew multiple domains manually close to expiration? Who will ensure your payment method on file is in good standing and that you have enough funds or a high enough credit limit to process critical domain renewals successfully? These are all decisions you will need to make based on your organization's particular requirements.

Once you have your tailored policies in place, you need to consider **how to consolidate your portfolio**. Should you migrate all your domains to a single registrar? Should you sell or terminate particular names that are no longer needed? What other gaps are there in your portfolio when compared to existing trademarks and brands? Should you purchase additional new TLDs or country code domains that have now come on the market? Questions like these abound for portfolio managers.

As a final consideration, you'll need to decide exactly how you will secure and police your domains. This is especially important for your most valuable domains, such as those that you have held the longest, attract the most traffic or have been used in various corporate marketing campaigns. Have you examined how you can protect domains that are administered in other countries? As domain attacks, cybersquatting and other exploits continue to increase in popularity and sophistication, this will be an important part of your overall strategy. A major part of your security effort will be ensuring that you keep your contact data current.

As you consider the complexities involved in formulating a domain portfolio strategy, you may begin to realize the value of a comprehensive domain management solution. Network Solutions offers such a solution with Platinum, an exclusive domain management service.

But before we dive deeper into this solution, it's important that you understand all of the challenges involved in managing a domain portfolio. Consider domain extensions.

Chapter 2

Deciding On Domain Extensions

Over the years, the Internet has become increasingly complex. The **days when dot coms ruled are over**. Back in the 1990s, if your company didn't own your dot com name, there weren't many alternative domain extensions. But now there are more than 1,500 options when it comes to TLDs. [4] These include AGENCY, .ARAB, .ASIA, .AUTHOR and .AUTO — and we're still at the start of the alphabet. There are other choices that involve using popular country codes (such as .ai, .tv, .io and .co) that have nothing to do with the country of origin of the domain owner.

In the early days of the commercial Internet, there were conflicts when common nouns were used by different companies as their own trademarks first and then as domain names. The simple resolution process used at that time — when there were just a few domain extensions — has been greatly complicated by the hundreds of extensions available now.

Having all of these domain choices is nice, but can be confounding. Should a business start buying up dozens of different domains to protect their brand's identity? What about hackers and criminals who want to extort money from a business by squatting on similar domains, or registering these newer extensions?

What is WHOIS?

The main way Internet domain specialists research and track domain ownership is through the use of the WHOIS lookups. If you are considering acquiring a new domain, you can check the WHOIS registry to determine if it's already taken. If it isn't and you want to register this new domain name, the Internet Corporation for Assigned Names and Numbers (ICANN) requires your domain name registrar to submit contact information to the WHOIS database that is maintained by your registrar. Once your listing appears in this online domain WHOIS directory, it is publicly available to anyone who chooses to check domain names using the WHOIS search tool, among other options.

In the old days, users would run queries to look up WHOIS information. Today, most people use WHOIS look-up sites or the website of domain providers, who are required by law to provide user-friendly WHOIS links on their sites.

Registrars offer ways to hide this information for an additional fee, and registrars have additional privacy features in certain instances based on applicable laws in the customer's country. This concealment is done by the registrar acting as your proxy — which means that anyone who does a WHOIS lookup for your domain name information will find the registrar's contact information, not yours.

Choosing the Right Tools

These traditional tools can be difficult to use for several reasons:

- First, because these tools have **non-obvious (or poorly designed) user controls**, they may make configuration or setting mistakes more likely. These mistakes could bring down servers or prevent sites from functioning correctly.
- Second, **not every IT administrator is familiar with the various settings and subtleties** of these tools. They are really for the ultra-specialists who use them frequently. Most IT departments don't have that level of familiarity with their commands and settings.
- Next, if **more than one person has access to these tools**, they could create conflicting configurations or negate each other's actions.
- Additionally, there is a **tedium of repeating common settings** for large domain collections, which makes mistakes likely and automation difficult to accomplish.
- Finally, if **multiple registrars are involved**, you might have to keep track of which tools are used to manage which domains.

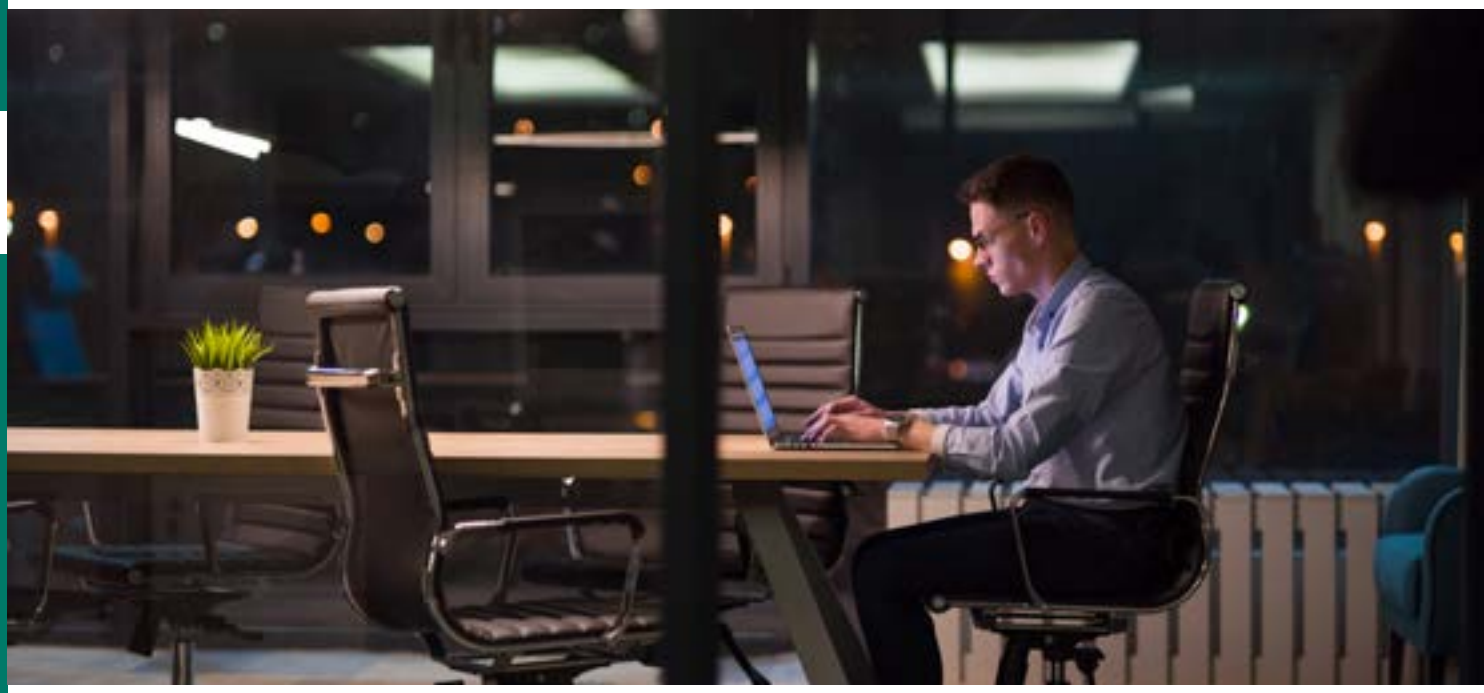
The Platinum Solution: Members of Network Solutions' Platinum service will work with experienced support personnel. These experts use the latest tools to help resolve potential domain issues, so you don't have to familiarize yourself with all the tools and deal with the ongoing tedium of using them.

The Role of DNS

Despite the importance of DNS, this protocol doesn't get the respect it deserves. Over the years, the DNS has been abused by spammers and had its weaknesses exploited by distributed denial of service (DDoS) attackers and domain hijackers. Most corporate IT staff don't spend much time maintaining their DNS services — typically when a business obtains a domain, they make use of the default DNS settings that come from the Internet provider. If these default DNS servers work, that is the first and last time that many of us think about our DNS. While that is the path of least effort, it is also the path of least functionality and protection. When something goes wrong with our DNS infrastructure, we might not have the technical chops to readily fix a problem: in the meantime, our Internet services could be offline. Mail Exchange (MX) records, which are another type of DNS record, also play an essential role by facilitating network communications (e.g., email).

This is why DNS is a critical resource. One survey [7] shows that an average DNS attack will cost an organization nearly $1,000,000. That is a huge potential downside. According to one 2019 IDG report [8], the number of DNS attacks is increasing. How a corporation maintains its DNS directly impacts how valuable its domain names will be. In this article [9], we talk about how it is time to get more serious about how you manage your DNS infrastructure and how you can harden it to prevent future threats.

An incorrect DNS parameter could be the reason your domain names are not resolving properly. There could also be some misconfigured services or settings. Fixing these errors can be daunting, even for the most technical IT staff who may not be trained or up to date on the latest DNS security protocols, as we describe in this article [10].



Registrar-Related Issues

Having registrars in control of domain ownership introduces some additional challenges for domain portfolio managers. First, domain transfer procedures remain somewhat complex and mysterious, as we describe in this eBook [11]. The process of finding and fixing errors in the transfer process can consume a great deal of time and technical expertise. This includes obtaining the necessary auth-codes [12] to move a domain from one registrar to another and entering these codes correctly and in the appropriate places.

There's also the possibility that you could be **unaware of those bad actors** who have registered domains with squatted addresses that are similar to your brands [13].

Unavailable domains could be already registered to someone else. Here is a very typical situation. Let's say your marketing department attempts to register a new domain name containing your company's trademark. However, the domain is currently being used by a third party that appears to be selling the same goods as your company. After extensive research and efforts by legal counsel, it turns out that the domain name was registered for official company use by someone in one of your own offices. This brings up our next point:

What third party uses or domain registrations could cause legal action from your company? Or what uses could cause your company to be named as a defendant in a lawsuit? The financial downside of these legal actions could be significant.

Finally, corporations may and often do use multiple registrars (and therefore need to connect with multiple WHOIS sources) or hosting providers, making their domain portfolios harder to track across the corporation and its subsidiaries. Using multiple registrars means that there needs to be someone keeping track of these domain renewals, so the domains don't expire without anyone being aware of it. Some of the worlds' largest corporations have dealt with embarrassing and untimely expirations. For example, Regions Bank is one of the largest banks in the United States, with over 1,700 branches and 2,400 ATMs. Yet they forgot to renew their domain name in April of 2013. Their websites were down for a week. (See other examples here [14].)

The Platinum Solution: Because of our extensive experience in the domains business, we are quite familiar with these issues. As a Platinum service member, you'll have a dedicated account manager to help you stay on track.

New and Existing Domains

The decision to purchase a new domain isn't a single or simple one. New domain names may not be needed at a certain time but could impact a company's brand equity in the future. There could be gaps or mismatches between the various trademarks your company holds and the domain names registered. You could also have a collection of domain names that reflect products that aren't part of your corporate assets or that you no longer sell. Ultimately, you need to make smart decisions about your corporation's portfolio so you can maximize its value. You need to be able to protect your corporate assets while also understanding that it isn't financially feasible to buy up every TLD. This means there are numerous domain-related decisions to make, such as which names to register, when to renew them and how often to evaluate your entire name portfolio.

Making matters more complex is that this cost-benefit calculation can differ depending on the names themselves. Calculating the potential costs of not owning a particular name – and the value of each name – is also more of an art form than a strict accounting process.

Next, **you need to know who is responsible for renewing or changing the existing domains**. Even if you can bring your legal, marketing and IT departments together, there is still a delicate balance of power that will be in effect once these existing names come up for renewal. That is because conditions can change that can influence the importance of those names. For example:

- When a competitor purchases a similar domain name to one of a company's existing brands,
- Your company expands into a new geographic market with different languages and alphabets,
- There have been legal challenges to your domain ownership or trademark battles or
- Criminals have launched various cyberattacks against your domains, including DDoS and domain squatting. An example of the latter is a homographic attack, which we discuss in more detail in this article [15].
-

The Platinum Solution: Dealing with both new and existing domains requires a balanced organizational response. The Platinum service can help you coordinate this response and make the right decisions.

Chapter 6

A New Standard

Defining your domain portfolio strategy isn't easy. There are many factors to consider and a number of perspectives needed to make informed decisions about your domains, including legal and technical views.

But good domain hygiene means more than being a technical or legal expert on domain ownership. It involves complete, top-to-bottom management of your domain portfolio, which, as you've seen throughout this eBook, isn't a simple task.

Fortunately, Platinum resolves this difficulty. This concierge service from Network Solutions is a complete solution for corporate domain portfolio management. You'll have a direct phone number and a single point of contact for managing your domains. Platinum membership includes:

- Brand protection strategies and customized recommendations.
- Mitigation against the risk of brand and trademark infringement.
- Quarterly business reviews.
- Bulk domain management and advanced configuration assistance.
- Assistance in maximizing your domain investment with security and strategies.
- Customized account statements and renewal notices.
- Priority issue resolution for any domain problems.

Ultimately, what defines the Platinum service is the time and money it saves you when it comes to domain portfolio management. With proactive, attentive service from responsive agents to remind you of expirations and renewals and in-depth technical assistance from domain experts, you'll be able to manage your portfolio with ease, sidestepping the many challenges we've outlined.

Simply put, Platinum sets a new standard for excellence in domain management. For protecting your brand, getting the most out of your domain portfolio and avoiding the stress and complexity of managing everything yourself, Platinum is the perfect choice. After all, when it comes to something as central to your business's online presence and success as your domains, why leave anything to chance? Trust your domain portfolio to the experts at Network Solutions. We'll take care of the rest.

End Notes

A COMPLETE GUIDE TO CORPORATE DOMAIN PORTFOLIO MANAGEMENT

1. http://robbiesblog.com/domain-names-owned-by-the-coca-cola-company/7013
2. https://www.techradar.com/news/these-companies-own-the-most-domains-on-the-web
3. http://www.dnsinstitute.com/research/fortune500-ipv6-201910/
4. https://www.wipo.int/pressroom/en/articles/2020/article_0026.html
5. https://data.iana.org/TLD/tlds-alpha-by-domain.txt
6. https://phoenixnap.com/kb/linux-dig-command-examples
7. https://www.techrepublic.com/article/how-dns-attacks-threaten-organizations/
8. https://www.efficientip.com/resources/idc-dns-threat-report-2019/
9. https://www.networksolutions.com/blog/data-privacy-and-security/how-to-evaluate-dns-security-providers/
10. https://www.networksolutions.com/blog/data-privacy-and-security/how-to-evaluate-dns-security-providers/
11. https://marketing.networksolutions.com/ip-block-selling-aftermarket-ebook/
12. https://www.icann.org/resources/pages/auth-2013-05-03-en
13. https://www.networksolutions.com/blog/data-privacy-and-security/protect-your-brand-from-domain-squatting-with-adultblock/
14. https://whoapi.com/blog/5-all-time-domain-expirations-in-internets-history/
15. https://www.networksolutions.com/blog/data-privacy-and-security/how-to-recognize-and-prevent-homograph-attacks/