Who Should Bear Domain Name Risk?

Alex Tajirian
September 28, 2008

Introduction

Domain owners are bearing tremendous risk that someone else is better equipped to absorb. In this essay, I outline the motivation of risk ownership, the sources of risk associated with owning a domain name, and the ways by which some of these risks have been transfered to institutions that are better equipped to handle them. I close by pointing out that we would be better served by having a trademark risk-management entity.

What is risk ownership?

Risk ownership[1] involves choosing which risks to bear and which to transfer or sell to another party. You should bear a risk only when you have the competancy to mitigate it or when there is no viable mechanism for transferring the risk. In general, the motivation for transferring risk is to reduce the overall risk for an individual or a business[2] and free up cash that would otherwise be needed as a cushion.

Risk management[3] is very important. Corporate success cannot be attributed solely to one person, but a single person or source of risk can indeed bring an established institution down. Nevertheless, risk management depends on the manager's appetite for risk.

Sources of Domain Name Risk

1. Domain Specific:
    a. Renewal. This includes forgetting to renew, not having the money to renew, and incorrectly deciding to renew[4] all domains in a large portfolio. The risk of forgetting to renew was initially born by the domain owner. Registrars soon realized they could make money by

---

[1] Robert C. Merton, "You Have More Capital than You Think," *Harvard Business Review* 83, no. 11 (November 2005): 84-94.
[2] Alex Tajirian (October 2005), "Domain Name Protection: A Risk-Analytic Framework," DomainMart.
[3] Risk management competency is one of the factors that should drive industry merger and acquisition decisions.
[4] See Alex Tajirian (July 2008), "To Renew or Not to Renew Your Domain Name?," DomainMart.

providing auto-renew services and encouraging discounts for multiperiod registrations. Registrar are better suited for owning this risk, as they can spread management cost over a large number of clients. Thus, the domain owner is willing to pay a fee for transferring the risk to a registrar.

b. Hijacking[5]

c. Trademark. Currently, a domain name is registered with prayers that no costly legal action will be taken against them. However, some of the new registrants take advantage of the system, while others innocently include brand names in their domain names. For the former, the cost of the illegal action is generally minimal, as they either surrender the domain name to the brand owner, don't pay for it before the end of the five-day grace period,[6] or possibly sell it at a high price at one of the prominent marketplaces.[7] On the other hand, the innocent group can be bullied into surrendering the domain name even when it does not legally infringe on someone else's IP, or they can incur uncessary shut down and legal costs. Hence, to manage this risk, the latter group should set aside cash to fight any potential legal action or if possible, transfer the risk to an entity that is better suited to absorb it.

   It makes sense that independent entities or registrars should sell trademark insurance policies. Such an intermediary must have legal expertise and the ability to spread risk management cost over a large number of clients. Currently there is no such institution, which implies that this risk is under-valued and thus represents inefficiency in domain name markets.[8]

   For trademark issues associating with existing domain names, a cooperative IP regime mitigates this risk and creates value to domain name owners and IP claimants.[9]

[5] See, for example, Bruce Tonkin (January 2005), "Closer Look at Domain Name Transfer Policy and the Hijacking of Panix.com," CircleID.
[6] See Alex Tajirian (August 2007), "Domain Tasting: A Solution," DomainMart.
[7] In such a case, the marketplace is an accomplice in infringing on the trademark, and thus the industry must take appropriate action against the marketplace.
[8] For marketplace inefficiencies, see Alex Tajirian (January 2006), "Price Inefficiencies in Domain Name Markets: An Empirical Investigation," DomainMart.
[9] See Alex Tajirian (April 2008), "Brand Complementors: Implementing a Cooperative Domain-Name Use," CircleID.

   d. Price risk[10]

   e. Parking Income[11]

2. Industry Wide
   a. General market price drop[12]

   b. Industry reputation risk requires domain activism,[13] lobbying by the Internet Commerce Association (ICA), and cooperation of domain name and trademark owners.
   c. Loss of privacy through public access to Whois information.

3. Sub-industry risk is due to front running,[14] potential bankruptcy and/or de-accreditation of registrars and resellers, and the risk of default of a secondary market player. Both these sources can disrupt activities for a segment of the market.

4. Transaction Risk
   a. Waiting too long to buy and/or sell. Thus, the risk of lost opportunities.
   b. Risk of money and ownership transfer, which can be mitigated by engaging an escrow agent.
   c. Ineffective domain-name valuation.[15]

5. Infrastructure risk[16]
   a. Spam and phishing
   b. Cyber security
   c. Lack of technology policy ■

[10] See Alex Tajirian (February 2006), "Toward Large Domain Name Portfolios," DomainMart.
[11] Ibid.
[12] See Alex Tajirian (February 2008), "Thoughts on Hedging Domain-Name Price Risk," DomainMart.
[13] See Alex Tajirian (July 2008), "Take Action: Your Domain Names Are Losing More Than You Realize!," DomainMart.
[14] See, for example, "Network Solutions Responds to Front Running Accusations," CircleID.
[15] See Alex Tajirian (December 2007), "Effective Domain Name Appraisals," DomainMart.
[16] See CircleID.