Domain Name Protection: A Risk-Analytic Framework

One of the important roles of corporate domain names is to protect the firm's intangible assets such as brand names, trademarks, and service marks.[1] However, the domain names, in turn, need to be protected.

Domain name risk arises when an entity acquires or leases a domain name. Taking and managing risk is part of what companies must do to create shareholder value. Thus, risk is a fact of business life.

A risk-based strategy is only one component of a successful value protection framework. The other success factor is a sound organizational structure to implement the strategy. Companies that fail to improve their domain name risk-management processes face the risk of severe financial loss.

Currently, there is no analytical framework to assist owners in determining the sources of domain name risk. The sources of risk are identified after a loss is incurred. An alternative, proactive strategy should go beyond identifying current sources of potential loss. What is needed is a strategy based on a comprehensive analysis of internal and external sources of risk. Identification of risk sources provides a basis for systematically examining changing situations over time to uncover circumstances that require close scrutiny.

[1] See Alex Tajirian, *Roles of Corporate Domain Names*, DomainMart.

Below, we focus exclusively on protecting an owner's domain names. We do not consider issues related to protecting a company's online identity nor presence.

PROTECTING THE PROTECTOR.
Currently, there is no universally agreed on definitions for the various sources of risk. The scopes of the sources of risk vary according to what best serves the particular problem being addressed. Thus, we describe each source separately and then suggest ways to group related factors.

Sources of Risk

1. **Operational risk** is the risk of monetary losses resulting from inadequate or failed internal processes, human error, and systems failure or from external events. Examples include:
    - Systems and technology failure
    - Inadequate document retention or record-keeping
    - Lack of supervision, accountability, and control
    - Data and modeling quality, such as appraisals
    - Fraud (internal and third-party)

    The consequences of mismanaged operational risk include domain name hijacking and failure to renew a domain name. These failures are not due to external threats; they are internal.

To mitigate this risk, companies must either improve internal organizational structure or outsource the management of this risk.

2. **Market risk** is the risk that general global economic conditions will affect returns of all assets, including domain names, in ways that are not anticipated. General economic and market conditions, such as interest rates, inflation rates, global economic uncertainty, and national and international political circumstances may affect value and price volatility of domain names.

   Market risk is a source of non-diversifiable external risk. Such risk, in principal, can be hedged using derivatives. The only financially viable domain name derivative is leasing. However, although a lease provides protection against downside risk, it does not allow the company to participate in the benefits from potential upside gains in value. To participate in the upside potential, the lease agreement must include an option-to-buy clause.

3. **Legal risk** is risk from uncertainty due to legal actions or uncertainty in the applicability or interpretation of contracts, laws or regulations. An example is when a company unknowingly registers a domain name that infringes on a third-party's trademark.

4. **Regulatory risk** arises when governments change the law in a way that adversely affects domain names. A recent example is the US government's pressure on ICANN to delay the final launch of the ICANN approved .xxx extension.

5. **Foreign exchange risk** is associated with foreign exchange fluctuations vis-à-vis, say, the United States Dollar (USD). This risk can arise when U.S. companies own or expect to purchase a large number of country domain names (ccTLDs) whose prices are fixed in country currency. Moreover, companies based outside the U.S. face some risk associated with registrations of .com names, as the registry fixes the price to registrars in USD. Nevertheless, unless the corporate portfolio of domain names is large, hedging this risk is not a financially viable option.

6. **Strategic risk** is that of a loss arising from poor strategic decisions related to domain names. For example, not preempting speculators and competitiors in registering strategic domain names. We believe that such an action is an internal source of risk and that brand managers should not blame external forces for their failure or for their asymmetric information. A second example of this risk is deciding whether to aggressively litigate perceived trademark violations or to acquire the relevant names. A third example of this risk is when a company registers domain names associated with future technologies, products, and services without concealing their identity. Such an action can provide valuable information to competitors.

7. **Business risk** arises from revenue volatility that stems from changes in industry demand and supply considerations or from competition.

Failure to deter speculators and competitors cannot always be achieved by preemption due in part to external forces in the registration allocation process. Also, changes in the scope and scale of the company's business can increase risk. One example of this risk is an increase in prices of domain name renewals.

8. **Reputation risk** is a consequence of damage to an organisation through loss of its reputation or standing. This risk arises when a situation, occurrence, business practice, or event has the potential to influence customers' and potential customers' perceived trust and confidence in a company. This risk can arise due to mis-managed strategic risk.

9. **Credit risk**, in general, is due to uncertainty in counterparty's ability to meet its obligations. This risk arises when a monetization service provider is unable to make obligations in full or on time. It also arises when a domain name lessee is unable to make a lease payment on time.

10. **Liquidity risk** arises from situations in which a party interested in trading an asset cannot do it because nobody in the market wants to trade that asset or when market participants have problems finding each other. Although, there is no trading invloved in protection per se, domain name acquisitons for protection are exposed to this risk.

ORGANIZATIONAL STRUCTURE

Organizational structure is a mechanism through which strategy is realized. It encompasses an organization's culture, people, and routines. Procedures and aligning incentives within the organization are also important for successful risk management. Thus, laying out protection rules is not enough.

IMPLEMENTATION

One way to outline risk management implementation is to map workflows to identify potential failure and associated losses.

Grouping of Factors

There is no unique criterion for grouping related risk factors. Groupings can be based on functional responsibilities within the company, the instruments used to mitigate risk, or sources of risk that must be mitigated.

Internal vs. Outsourcing

The company also has to decide whether to manage risk internally or to outsource it. This decision should be based on the company's competencies and its risk tolerance.

Measurement

The risk can be quantified by calculating expected loss for each risk factor. Value at Risk (VaR) can be used to measure the downside risk of the portfolio of domain names.

Alex Tajirian
CEO

Related Articles: Corporate Domain Acquisition Strategy

Related Services: Corporate Domain Management (CDM)