Figure 26-7: Potential Searchable Whois Forms of Abuse and Mitigation. *Verisign leverages its experience supporting the .name registry to build in to the system the safeguards necessary to minimize abusive Whois practices.*

Potential Abusive Searchable Whois Risks	**Verisign Risk Mitigation**
Single Source Data Mining The mining of Whois data from a single IP address conducted through manual queries	Access Control Lists (ACL): Implementation of an ACL at the network layer to block the offending IP address for a specified period of time; viable option given a single unique IP address Application Rate Limiting: Implementation of rate-limiting at the application layer to regulate the number of queries allowed from the source IP address for a specified period of time; viable option given a single unique IP address
Automated Data Mining Single Source: The mining of Whois data from a single IP address conducted through the use of automated scripts Distributed: The mining of Whois data from multiple sources/IP addresses conducted through the use of automated scripts, or, "botnets"	ACL and Application Rate Limiting as defined for single source data mining Packet Inspection: Implementation of tools that analyze the incoming "get" request to determine whether the source is a valid user or whether the request is coming from an automated script or botnet; viable option based on "get" request signature Completely Automated Public Turing Test To Tell Computers And Humans Apart (CAPTCHA) Techniques: Implementation of a challenge-response test prior to processing the request; viable option that limits ability to predict challenge-response; almost always requires manual interaction