

DIGITAL DUE DILIGENCE QUESTIONNAIRE

- Do you have an online monitoring system in place?
 - Does this include monitoring blogs, message boards, Twitter, Facebook, message boards, comments posted to online mainstream media articles, YouTube and other relevant communities and channels?
 - Is someone regularly checking in on historical online posts that might have been negative or a previous online crisis situation to make sure nothing new is developing?
 - Are you subscribed to industry-specific blogs and Twitter accounts?
 - During any crisis, stakeholders' first destination online will likely be their favorite search engine. Do positive brand-related items appear in the top ten search results for a search query about your brand or other relevant searches?
- To what extent does the organization monitor? Real-time, Hourly, Daily, Weekly, None?
- Are there digital or social media components included within your crisis communications plan?
 - Does the plan include scenarios with social media components?
 - Does the plan define what might be considered an online crisis?
- If you have organizational accounts set up on popular social media communities/channels do you have a specific crisis plan or framework in place should an issue arise? Do you regularly hold crisis simulations to put these plans/frameworks into practice?
- Do you have an online engagement protocol that helps set an organizational framework or guidelines for when to respond online?
- Are your employees active online? If so, does your organization have an employee social media policy/protocol/guidelines?
 - If yes, have employees received training on the policy/protocol/guidelines?
- Do you currently maintain a dark or an issue-specific micro site to facilitate indirect and direct inquiries during crisis scenarios? If no, do you have a plan to escalate "dark" content on your main website during a crisis situation (i.e., when to put something on the homepage and a protocol to do so)?
- Do you already have pre-established relationships with key online influencers (e.g., bloggers and community moderators)? Is there someone responsible for fostering these relationships and who serves as an individual point-of-contact?
- Do you own your brand URLs in the around the world? Including country domains and popular domains like .org, .com and .net, among others.
- Do you own common negative brand URLs (e.g., brandXsucks.com or URLs tied to specific issues like lawsuits or your CEO/Chairman/President)? Do you own other relevant pre-registered URLs that might be able to help during a crisis (e.g., brandXresponds.com or brandXfacts.com)?
- Have senior managers gone through a basic social media 101 class or briefing to understand the fundamentals of online communications, including transparency, authenticity, genuineness, conversation, openness, completeness, etc.?

- Do you have accounts set up or work with a partner who can quickly turn on online advertising or a search engine paid keyword advertising campaign?
- Do you proactively publish useful, positive information online? Are you already active in social networking communities?
- If you are a global organization do you have a plan to coordinate online crisis monitoring and response efforts around the world and across multiple time zones and languages?
- Does your crisis response team or crisis management team include a representative from the legal department that has been trained or understands the fundamentals of online communications and past legal examples of best and worst practices when dealing with legal issues online?
- Do you include digital or social media elements into crisis training and simulations?
- Have you done crisis training or simulations for every new social media channel you launch?
- Are your community managers for social media channels formally trained like company spokespeople are?

Dan Webber
Executive Vice President, Digital Crisis Management, Edelman
202-772-3562
Daniel.Webber@edelman.com