CORPORATE REPUTATION and INFORMATION MANAGEMENT

AUTHOR: JOHN L. HINES, JR.
CLARK HILL PLC

A reputation management program may be the most important element of an information management strategy. Indeed, it may provide an organizing principle for other components of a total information management policy. To understand why this is the case, and what the components of an information management policy are, it is necessary to understand a little about the taxonomy of information.

Information: The Corporate Landscape

Information may have first or second level significance. Corporate artifacts, things, documents and data can have independent, operative, self-revelatory, first order significance. First order information may include information that is embedded in, and thereby conveyed through, the company's products, inventions, other intellectual property, policies, processes and contracts. These materials reveal significant operative information in the "thing" itself. The operation of a factory reveals material information in its operation—its methods and processes. The machines, to the extent they are patented by and/or for the company, reveal material information about the company and that information may be protected by applicable intellectual property laws. Contracts between vendors, suppliers and contractors may have first order significance as establishing the web of relationships constituting the valuable supply chain.

The bulk of corporate information consists increasingly, however, in information of second order significance embodied in documents, messages or other data about the corporation and often in immaterial ways (e.g., lunch invitations). Corporations store a staggering amount of such information.

When thinking about the landscape of corporate information, it is also useful to think about information that is (i) at rest or (ii) in transit as a message. Information at rest is information that is embedded in the self-revealing operations of the company or information about the company that is archived in the memories of individuals, on company systems and devices, or on third party systems, including those of cloud providers. Information in transit includes messaging to and from employees of the company, to and from employees and third parties, and to and from third parties.[1]

Information: A Significant Source of Enterprise Value

Corporate information in all of its various manifestations may be thought of as an intangible. The element of control determines whether information is an asset or a liability. When the company successfully controls information and harnesses it for useful corporate ends, it may be thought of as an asset. When the corporation fails to control the information, the intangible becomes a liability.

Controlling information—turning an intangible into an asset—has potentially significant consequences for enterprise value. According to Ocean Tomo, "Within the last quarter century, the market value of the S&P 500 companies has deviated greatly from their book value. This 'value gap' indicates that physical and financial accountable assets reflected on a company's balance sheet comprises less than 20% of the true value of the average firm."[2]

While organizations and information technologies can create great efficiencies, the more that corporate systems and devices grow and proliferate, the more entropic is the information that passes through those systems and organizations, i.e., the more the information seems to look "for a way out" and be "free." Technology systems as they get larger and capable of performing more tasks tend to become more vulnerable to intrusion—leading to increasing efforts at security and "appliancization" (rendering the technology less open, more task specific and thereby less vulnerable).[3] The growth of organizations and of information systems presents special challenges for information management.

Controlling Information: Information Management Policies

Companies should establish a suite of information management policies to combat the entropic quality of information. These policies should be created, maintained and overseen by a committee with representatives from at least the following departments: corporate, legal, finance, security, compliance, IT, marketing and HR. The policies include:

1. Corporate handbook and code of conduct: generally governing the principles of corporate responsibility and good citizenship (establishing corporate ethics and sustainability);
2. Employment policy: generally governing principles relating to proper intra-corporate behaviors, including safety, anti-harassment and anti-discrimination;
3. Quality assurance manual: governing processes for assuring quality of products and/or services;
4. Intellectual property policy: governing ownership and rights relating to innovation, inventions, creative works, proprietary information, and use of marks;
5. Communications policy: governing use of computers, mobile devices, telephones; media commentary and public relations; use of Internet and social media; use of company name and brand; communications relating to company products; public and media relations; and employee expectation of privacy in use of corporate systems;
6. Privacy policy: governing the collection, use and transfer of information from third parties and employees with emphasis on information that is personally identifiable to an individual or reasonably identifiable to a particular device;
7. Security policy: governing information security in whatever media, whether at rest or in transit, with emphasis on access controls, perimeter controls, and encryption of data at rest and on mobile devices; protocols in the event of a security breach; and,
8. Document retention policy: rationalizing information storage and governing the retention and destruction of documents, whether on intra-corporate systems or stored through cloud providers.

The information management committee members must work closely together in establishing, monitoring, and enforcing the policies and, importantly, on appropriate training. For example, if IT wants to move certain systems to the cloud, the systems transition will involve regulatory considerations depending on the location of the servers, the security offered by the provider and the relevant data protection laws. The project will involve integration with applicable records retention policies, including managing litigation holds, and relevant HR considerations relating to storage and transmission of sensitive information. As another example, if marketing and sales are planning on offering new customer login opportunities on social media sites, this decision may involve a cascading set of information management consequences that

require input from multiple corporate sectors. The decision may involve access to your customers' personal information by the social media site or by a set of new advertisers, which may mean additional disclosures in your privacy policy-- all of which involves IT, legal, marketing, sales, privacy and security.

The point is, corporation operatives must be trained to recognize the significance of collection, transfer and retention of information and report to the committee (or responsible delegated parties) any changes in practices.

Reputation: The Cornerstone of Information Management

These policies present a process for controlling information and turning the body of corporate information into a strong intangible asset.

> *The compilation of beliefs and perceptions that key reputation stakeholders have in the strength of the values and processes defined by these policies is in large measure the reputation of a company. More specifically, reputation is a function of the key stakeholders' perception of critical business intangibles, including ethical and legal compliance, innovation, quality, safety and security.*[4]

These business intangibles and behaviors are the very ones that are fostered by the policies described above. Key stakeholders in reputation creation include employees, vendors, customers, shareholders, competitors in the industry, individual and corporate geographic neighbors and, to some extent, the public at large. The greatest way to assure a strong reputation is, of course, to implement and secure, as much as possible, compliance with the policies.

It follows from the above that reputation provides an organizing principle for a total information management policy. A corporation striving for a good reputation necessarily must strive to achieve the processes fostered by the eight policies above—and this will have measurable economic consequences. A strong reputation will "pay off with (i) pricing power, (ii) lower operationg costs, (iii) greater earnings multiples, (iv) lower beta (i.e., stock price volatility) and (v) lower credit costs." [5]

Maintaining Reputation Has its Own Unique Challenges

Nevertheless, there is not a complete correlation between the eight policies and a good reputation. This is because reputation is by definition a function of beliefs about corporate behaviors, and these beliefs themselves may be based on second order communications from people who have only remote connections to the corporation. The beliefs of reputation stakeholders may not reflect the facts or may be based on an out of date or misleading rendition or interpretation of the facts.

This disconnect between belief and fact is further complicated by web based and mobile technologies and by social media where communication at no cost is now viral, transparent, permanent and infinitely searchable. A corporation's reputation is now largely the composite of what shows up in search engine results, rating sites, chatter on the myriad of websites, blogs and other social media sites – in addition to that appearing in traditional media.[6] True, false, misleading or out of date information about a company can be published at no cost and distributed instantaneously. Further, the ecology of information transfer includes human belief systems that are prone to "following the herd" and tend to bias towards existing prejudice, notwithstanding actual facts.[7] Add to that the public's new willingness to say things under the cloak of anonymity that it might not have said in the pre-Internet days and a new body of law that, while it has admirably promoted the interests of the First Amendment and a robust Internet, has arguably offered little in the way of protection to the victims of negligent or defamatory speech.[8]

Examples of corporations being hit literally in an instant by an event discrediting ethics, security, product quality or any other of the components of reputation are legion.[9] Once a discrediting event hits, the information about the event may find its way to the first page of Google, and once there Google's algorithm tends to reinforce the story based on popularity rather than truth.[10]

Corporate stakeholders should thus undertake additional measures to manage reputation. These measures would ideally include the following:

1. Play offense on social media. Create a robust presence with content that tells a compelling and truthful story about your corporation. This strategy may involve creating profiles on relevant social media sites, asserting control of relevant domains with the same or a similar name, creating content on relevant websites and where possible creating links to and among your various web presences. This strategy may prove helpful in creating a healthy presence, controlling your corporate identity in the face of third party chatter and in eclipsing inaccurate or even defamatory comments that otherwise could prove harmful (because, for example, it shows prominently on Google). In short, if you don't control your corporate identity and the messaging about your company, someone else will.[11]
2. Have in place a crisis management team and a game plan if and when something happens. The team may include outside PR consultants and experts in online profiling and search engine and rating site optimization. You may want to have a site/blog ready to activate that is designed to create appropriate messages to the public in dealing with the particular crisis. And be prepared to use social media (e.g., YouTube, Twitter and Facebook) to broadcast your message. Crisis management will be more or less successful depending on the speed and quality of the messaging efforts. Again, negative reputational events in the digital world can have, in some instances, immediate consequences on consumer demand and stock price.[12]
3. Consider your overall reputation strategy and the elements of reputation that are particularly important to your customers, investors and other reputation stakeholders in your particular industry. This of course may involve complex questions of business ethics in how one rationalizes conduct that is clearly beneficial to society, but perhaps less beneficial to immediate stakeholders.
4. Consider reputation and other relevant cyber-insurance. The arena of risk management insurance policies covering reputation exposure is an evolving area. Potential areas of coverage may include crisis preparedness (including event training), crisis management and loss of value.[13] Companies should also consider the availability of insurance policies that may insure over risks related to the underlying components of reputation. For example, some carriers are now offering insurance for certain risks associated with a security breach and the compromise of personal data. Companies are well advised to confer with their risk management professionals about the possibility of relevant coverage.

1 And, again, messaging may be in a variety of forms including, for example, advertising, email or information embedded in the distribution of products as they appear in the marketplace.
2 See, http://www.oceantomo.com/productsandservices/investments/intangible-market-value; Ocean Tomo reports that a significant portion of the intangible value reflected in its study is represented by patented technology.
3 Jonathon Zittrain, "The Future of the Internet and How to Stop It" (Yale 2008).
4 Dr. Nir Kossovksy with Todd A. Miller, Mission Intangible: "Managing Risk and Reputation to Create Enterprise Value," p. xxi (Intangible Asset Finance Society 2010) ("Mission Intangible");
5 See Id. at 8, 30-31,165.
6 Michael Fertik and David Thompson, "Wild West 2.0: How to Portect and Restore Your Online Reputation on the Untamed Social Frontier" (Amacom 2010), 16-29 and 150-161 ("Wild West").
7 See, Cass R. Sunstein, "On Rumors: How Falsehoods Spread, Why We Believe Them, What Can Be Done." (Farrar, Straus, and Giroux 2009). As Winston Churchill supposedly said, "a lie gets halfway around the world before the truth has a chance to get its pants on."
8 Section 230 of the Communications Decency Act, enacted in 1996, immunizes service providers, blogs, websites and other intermediaries that carry the information created and developed by others. 47 U.S.C. § 230(c); See, Zeran v. AOL, 129 F.3d 327 (4th Cir. 1997). Analogous offline publishers do not have such an immunity. Moreover finding the speaker and/or piercing anonymity presents equal challenges. See, e.g., Dendrite v. Doe, 775 A.2d 756 (N.J. App. 2001).
9 See generally Mission Intangible and Wild West.
10 Wild West at 84-85.
11 Wild West, at 188-206.
12 The author thanks Jonathon DeMay for his comments on this point.
13 The author thanks Pamela Newman for her comments on this topic.