Guarding the Social Gates:

The Imperative for Social Media Risk Management

August 9, 2012

By Alan Webber

With Charlene Li and Jaimy Szymanski

Includes input from 42 ecosystem contributors

Executive Summary

Social media is the modern Pandora's box: It has had a meteoric rise as a tool to interact and engage with customers, but also a dark underside exposing companies to new types of risk. Almost two-thirds of companies surveyed say that social media is a significant or critical risk to their brand reputation; yet 60% of companies either never train their employees about their corporate social media policies or do so only upon hiring. Moreover, 43% of companies have less than one Full-Time Equivalent (FTE) dedicated to managing social media risk.

To safeguard brand reputation, protect information and intellectual property, and mitigate legal actions, organizations need to be more proactive about managing social media risk. To set up an effective social media risk management process, organizations need to focus on: 1) identifying social media risks; 2) assessing and prioritizing those risks against limited resources; 3) mitigating and managing those risks to reduce the impact on the organization; and 4) evaluating emerging risk against mitigation efforts.

Methodology

For this report, Altimeter Group conducted both quantitative and qualitative studies using a combination of an online survey, qualitative interviews, and an analysis of publicly available information. Specifics include:

- This year we launched the *2012 Altimeter Social Media Risk Management Survey*, an annually updated online survey and organizational assessment on management of social media risks. For 2012, we surveyed 92 professionals from various industries and backgrounds who, in their current professional roles, said that social media risk management was their primary job function or a significant part of their professional responsibilities.
- Qualitative interviews with 36 companies. Roles interviewed included: social media managers, compliance officers, lawyers, Chief Security Officers (CSO), social media risk managers, and senior executives of vendors, agencies, and end users.

Table of Contents

Social Media Often Has Unrecognized Risks

Organizations today are jumping on the social media bandwagon in record numbers. In the United States, more than 80% of companies have a presence on Facebook, and 45% are active on Twitter.[1] Globally, approximately 16% of companies are using social media to interact and engage with their customers, according to the *2012 IBM Global CEO Study*, and that number is expected to triple in three to five years.[2] More organizations are using social media to reach and engage with customers and potential customers.

It sounds like a panacea, but social media isn't all Eden. Imagine the 1:35 a.m. call informing you that your new product scheduled for release next week has been accidentally leaked because of some Flickr images. Or the 5 p.m. call that the regulators are going to be in your office first thing tomorrow because of a response that one of your customer service reps tweeted to a customer. These are not hypothetical examples, but some of the real incidents that have happened to companies in the past year that keeps social media managers, CMOs, compliance officers, and others up at night wondering if it could happen to their organization.

Companies are often aware of the risks at some level, but instead of taking specific concrete actions, they cross their fingers and hope that they dodge the bullet. The result: A whole new aspect of risk is introduced into the business equation — social media risk.[3] Altimeter defines social media risk as:

> *The likelihood that a negative social media event will happen*
> *(multiplied by)*
> *The impact that negative event will have if it does happen*

Defining the Types of Social Media Risk

To find out the perspective organizations have on social media risk, we interviewed 33 people who are involved in social media and social media risk management. We also surveyed 92 professionals who said that social media risk management was their primary job function or a significant part of their professional responsibilities. When it comes to social media, we found that the perception among most companies is that though social media is a valuable addition to the organization in areas such as marketing, customer support, customer engagement, and internal collaboration, it also presents potentially significant risks in areas like brand reputation, employee productivity, and malware (see Figure 1.1).

Specifically, we found that the four largest risks perpetuated by social media are:[4]

1. **Damage to brand reputation.** Of those surveyed in our *2012 Altimeter Social Media Risk Management Survey*, 66% of 52 companies told us that social media represented a significant or critical risk to the reputation of the organization. Damage to brand reputation can result in a loss of trust or credibility of the organization. For example, the tweet by Kenneth Cole in February 2012 about the uprising in Egypt: "Millions are in uproar in #Cairo. Rumor is they heard our new spring collection is now available online at http://bit.ly/KCairo – KC" did significant damage at the time to the brand.
2. **Releasing confidential information.** Whether accidental or malicious, by its very nature social media can facilitate the inadvertent release of information. Companies are constantly concerned about the leakage of confidential information, from earning indications to changes in key staff. Of those we surveyed in our *2012 Altimeter Social Media Risk Management Survey*, 32% of 52 companies told us that social media was either a critical or significant risk to releasing confidential information. For example, Gene Morphis, the former CFO at Francesca's Holdings (a fashion retailer and public company) was fired after tweeting confidential information such as "Board meeting. Good numbers=happy board" and "roadshow completed. Sold $275 million of secondary shares. Earned my pay this week."[5]

3. **Legal, regulatory, and compliance violations.** While the government works with private industry to reformulate its regulations around social media, companies in highly regulated industries want to engage and, at the same time, not violate any laws or regulations. For example, regulators fined Australian company Allergy Pathway for misleading testimonials written by its fans on Facebook and Twitter, even though Allergy Pathway did not write them.[6] That is the reason 30% of 52 companies we surveyed in our *2012 Altimeter Social Media Risk Management Survey* indicated that the legal, regulatory, and compliance risks from social media were critical or significant, while another 25% rated the risk as moderate.

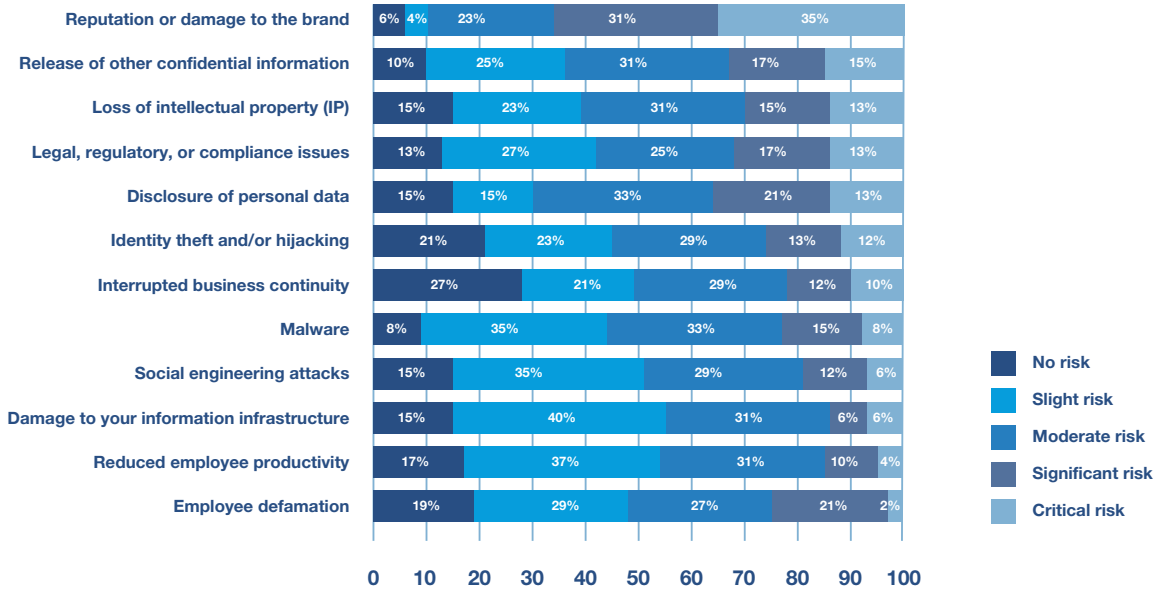
4. **Identity theft or hijacking.** Unfortunately, people having their identity maliciously stolen or hijacked is a common news story. Becoming more common are organizational identities being hijacked on social media platforms, including setting up fake Facebook pages or Twitter feeds and providing false information or acting otherwise maliciously. For example, anti-brand Facebook pages, user-created ads, and tweets were recently used against Royal Dutch Shell concerning its drilling in the Arctic.[7] The effort, believed to have been executed by Greenpeace, includes a believable website, the ability to create ads by users, and the functionality to employ social media channels to spread the hoax. Brand hijacking and traditional identity theft fears led 25% of 52 companies we surveyed in our *2012 Altimeter Social Media Risk Management Survey* to say that they felt the risk was critical or significant.

The Most Popular Platforms Are Also the Most Risky.

While companies are aware that social media creates risk and that it is growing, that risk is not equal across platforms. Different platforms offer different levels of audience reach, different types of engagement, and different levels of interaction. When asked, organizations see a significant portion of the risk tied up in just a few of the primary platforms (see Figure 1.2).

Figure 1.1: Damage to Brand Reputation is the Largest Risk

"In the following areas, what is the level of risk that social media currently presents for your business?"

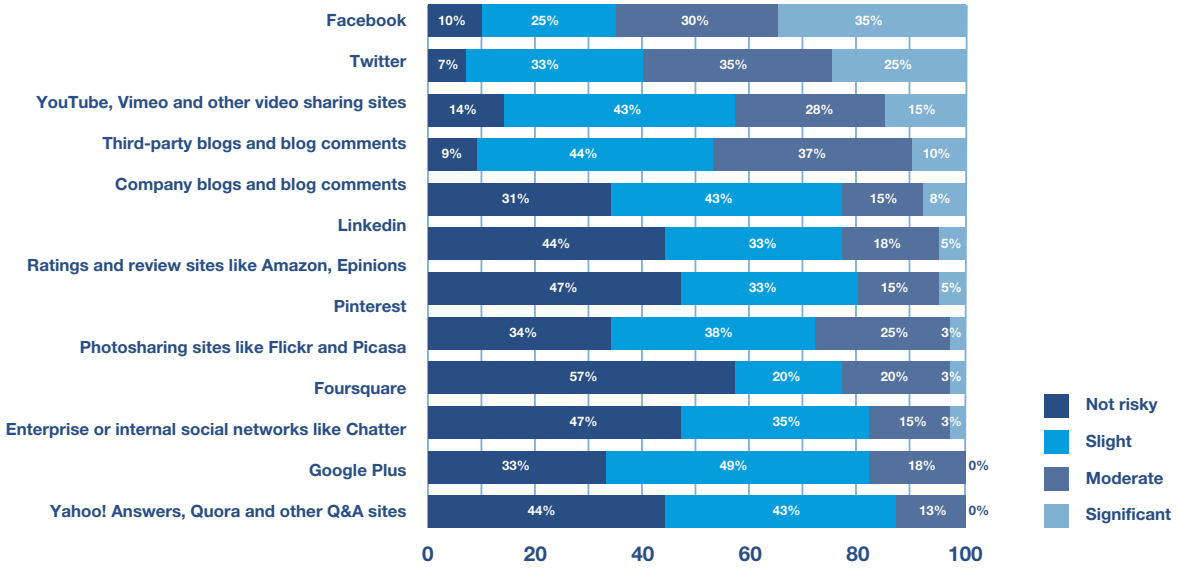


Note: Answer percentages may not add up to 100%, due to rounding.
Base: 52 of 61 respondents for whom social media risk management is their primary or a significant part of their responsibility.

Source: "Guarding the Social Gates: The Imperative for Social Media Risk Management," Altimeter Group (Aug. 9, 2012)

Figure 1.2: The Most Common Social Platforms Are the Primary Sources of Risk

"How risky do you currently consider the following social media channels to your organization?"



Note: Answer percentages may not add up to 100%, due to rounding.
Base: 41 of 61 respondents for whom social media risk management is their primary or a significant part of their responsibility.

Source: "Guarding the Social Gates: The Imperative for Social Media Risk Management," Altimeter Group (Aug. 9, 2012)

ALTIMETER

Specifically, companies told us that:

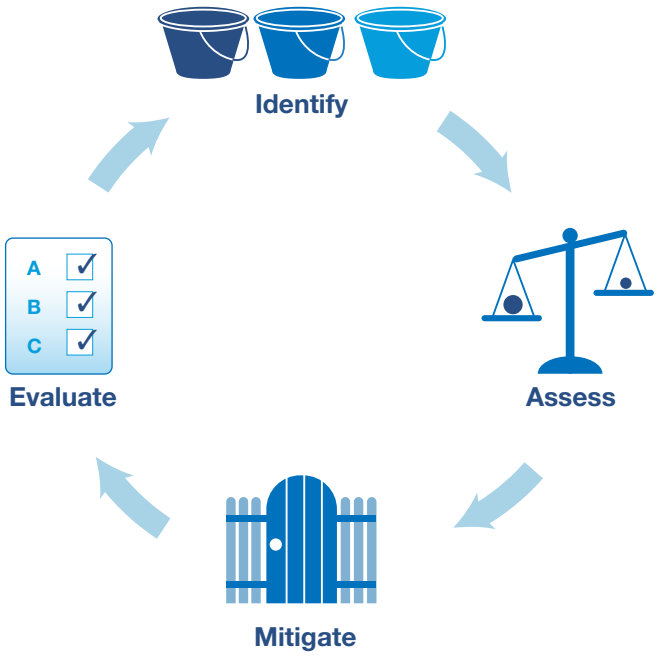
- **Platforms with the broadest reach are the largest potential risk.** When it comes to assessing the top sources of risk, risk managers turn no further than the big three — Facebook, Twitter, and YouTube. Of those we surveyed in our *2012 Altimeter Social Media Risk Management Survey*, 65% of 41 companies told us that Facebook was a moderate or a significant risk, 60% felt the same about Twitter, and 43% felt that way about YouTube and other video sharing sites. Of all of the social media platforms, these three have the broadest reach, visibility, and adoption among consumers, which all contribute to a higher level of risk. But there are additional factors, such as the frequency of change in the platform and the lack of control over the platform by a brand. For example, more than one company we interviewed said that the frequent privacy policy changes on Facebook left them open to increased risk until the company had a chance to assess the policy and adjust accordingly.
- **Lack of control is a significant source of risk.** When asked about third-party blogs and blog comments, 47% of 41 companies we surveyed in our *2012 Altimeter Social Media Risk Management Survey* indicated that these platforms are a source of either moderate or significant risk. Third-party blogs and blog comments reside outside the span of control of the organization and are places where people and groups can freely express their opinion about an organization with few repercussions. In some cases, these blogs can have significant followings with key customer constituencies for a brand. A great example of this was the Heather Armstrong (@Dooce on Twitter) social media crisis for Whirlpool, where the dissatisfied "mommy blogger" turned out to be very influential in the brand's primary customer space.[8]

Putting a Social Risk Management Process in Place

Organizations have limited resources. Without understanding what levels of social media risk exist, it is impossible to prioritize which risks to position resources against for control and mitigation.

Organizations can choose to shift from being reactive to proactive. The best ways for organizations to become proactive and reduce the impact of a social media crisis is to have a social media crisis management process in place. Social media risk management is a process of evaluating tradeoffs, essentially a cost benefit analysis, as you work from the highest priority risks to the lowest priority risks. We have identified four distinct steps to social media risk management (see Figure 2).

Figure 2: Risk Management IAME Loop



Source: "Guarding the Social Gates: The Imperative for Social Media Risk Management," Altimeter Group (Aug. 9, 2012)

ALTIMETER

This process, once established, should become a cycle in which the organization has a systematic effort to continually evaluate the social media risks it faces and its responses. In more detail, the four steps of social risk management are:

- **Identify the Risks.** The first step is to identify potential risks that can be manifested through social media. These can be risks that are created in the social channel, such as a negative campaign by an activist organization, or the risk that the social channel will amplify a situation or incident. Almost every company we spoke with used a listening platform, such as Radian6 or Crimson Hexagon, as one way to identify potential social media risks. But beyond listening, other companies also ran "brainstorming" sessions where they looked at recent social media and brand crises and then assessed if and how the same scenarios could happen to them.

- **Assess the Risks.** In this step, organizations assess, evaluate, and prioritize risks against the likelihood that they will happen and the potential impact if they do occur. At a base level this can be a qualitative analysis, but at a more advanced level this should be a quantitative analysis. Most of the companies with whom we spoke used a very near-term and ad-hoc assessment process; basically, they didn't begin to assess a risk until it was already beginning to manifest and, then, only using a simple qualitative process. Other companies in more regulated industries use a more structured risk-assessment process, including bucketing the risk, assigning a set of values to each risk and the likelihood of manifestation, and then prioritizing those risks based upon the assessment.
- **Manage and Mitigate.** In this step, organizations implement mitigation, management, and control efforts, beginning with taking an inventory of what current management and control tools are already in place. Almost every company we spoke with employed either one or more mitigation strategies, including policies, compliance technologies, and employee training. For example, Dell has a robust social media training effort that allows employees to become social media advocates for Dell.
- **Monitor and Evaluate.** The social media risk landscape is in a constant state of change. For that reason, organizations should regularly review and evaluate their current social media risk control efforts, update the inventory of social media risks, and put new mitigation and control processes in place.

Step 1: Identify the Risks.

The first step in social media risk management is identifying which of the categories of risks your organization faces. Eddie Schwartz from RSA, the security division for EMC, put it very succinctly: "You can't use 'chase and respond' as your approach to social media risk management. It all has to be about going out and finding where your weaknesses are, what threats exist, and who your adversaries are — all proactively."

Understanding how social media risks can be categorized can help to more effectively assess, manage, and respond to these risks. We have broken them down into four general buckets based upon how, if perpetuated, they affect the organization. These four buckets are:

- **Organization reputation.** Damage to brand reputation can cause a loss of trust or credibility that can result in either potential or real financial loss. For example, the tweet by online clothing boutique www.CelebBoutique.com, "#Aurora is trending, clearly about our Kim K inspired #Aurora Dress" not long after the deadly movie theater shooting in Aurora, Colorado, will likely result in lost sales to the company.
- **Regulatory and compliance violations.** Regulatory and compliance risks are those risks that, if an organization posted on a social media channel, it could be in violation of a government regulation that could result in financial and/or other penalties. For example, the Federal Drug Administration (FDA) admonished Novartis for its use of the share widget on its Facebook page promoting the drug Tasigna, which is a violation of FDA advertising guidelines.[9]
- **Legal and privacy.** Legal and privacy risks are the result of an organization failing to take an action — such as effectively safeguarding personal information — that could cause harm to another party. Often, employee- and human resources-based risks or privacy issues, such as releasing confidential personal information, fall into this bucket. For example, when Dr. Alexandra Thran posted on Facebook about the patients she was seeing during her clinical training, but didn't post their names or other identifying information, she thought she was fine. But then, a third party was able to figure out who one of the patients was based upon the injuries she posted about it, and Dr. Thran was fired for violating patient confidentiality.[10]

- **Operational.** Operational risks are those risks that could compromise the overall operations and security of an organization. Operational risks can be further broken down into five sub-categories: 1) reduced employee productivity, 2) release of confidential company information or IP, 3) the introduction of malware into an IT system via a link on a social platform, 4) direct attack toward employees and principals, such as a social engineering effort, and 5) business continuity on primary digital business channels, such as an e-commerce platform.

No risk falls into a single category, as every incident that manifests takes on unique characteristics that cause it to cross categorization boundaries. For example, an accidental release of private customer information by a financial services firm would start as an operational risk and then move to a regulatory risk when the incident is reported to the appropriate regulatory agency. It then becomes an organization reputation risk when the data loss becomes public, and lastly it evolves into a legal risk if one of the customers whose data was compromised decides to sue.

Social media threat identification is a continuous and ongoing process that is unique to each organization. That being said, the more advanced organizations we spoke to took a two-tiered approach that had both continuous and incremental reviews, with continuous reviews happening on a weekly to monthly basis and deeper and more intense reviews happening on a quarterly to annual basis. To identify potential social media risks, more advanced companies use a combination of the following activities.

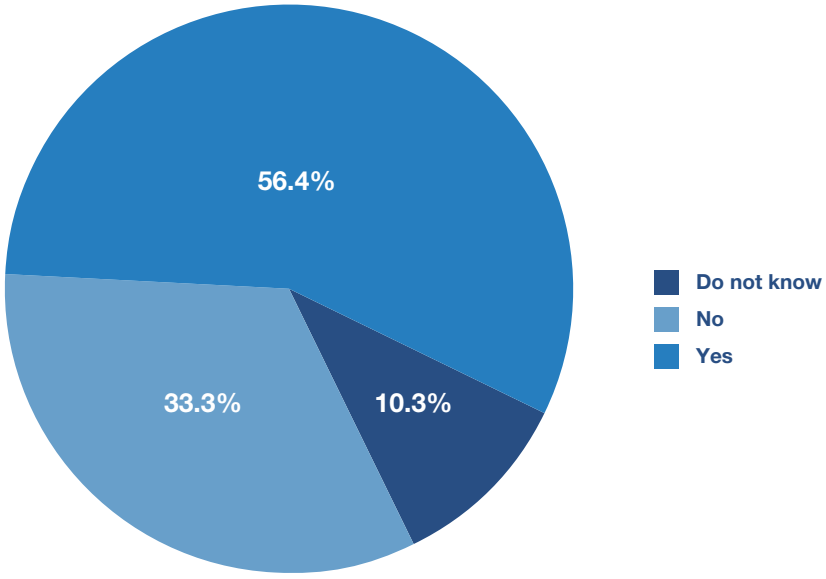
1. **Review historical activities.** As one company pointed out, social media risks, like other risks, tend to follow patterns. One way then to identify social media risks is to examine how the company has suffered an adverse impact previously in both traditional and social channels.
2. **Scrutinize what they are hearing through listening.** Many companies look for new risks popping up across their listening platforms on a continuous basis and classify those risks as either immediate or long-term. Immediate risks are pushed into a crisis management process, and the lower level, long-term risks are moved back into the risk-assessment process.
3. **Learn from others.** There are social media crises and incidents happening all of the time, and each of these events are great learning opportunities for companies. One company we spoke with has a multi-disciplinary team that does a weekly analysis of the news, looking for case studies and newly identified risks that are then put into their risk-assessment process.
4. **Create a social media risk library.** Several of the companies we spoke to are creating or have created a library or list of potential risks — similar to what Intel created in the Intel Threat Agent Library — and adding to these as they are identified.[11]
5. **Review new activity risks.** Every time a team or a division of a company wants to start a new social media activity, these activities should be reviewed for exposure to new risks. For example, when the customer service team of a large financial services firm wanted to launch a new customer service effort via social channels, the activity was closely examined for potential risks.
6. **Examine shifting platform risks.** Lastly, platforms are constantly changing, and companies that essentially "rent space on these public platforms," as one company put it, need to review those changes for potential risks. The firms we interviewed mentioned some of the more common platform changes that shifted their risk exposure, including changes in privacy policies, changes in data retention policies, and changes in the actual functionality of the platform itself (such as when Facebook introduced Timeline).

Step 2: Assess the Risks.

Many companies don't know what level of social media risk they're taking on, because they don't regularly assess and quantify their social media risk. We found that 56% of 39 companies we surveyed in our *2012 Altimeter Social Media Risk Management Survey* regularly assess their social media risk (see Figure 3). In our interviews, companies expressed numerous reasons for not regularly assessing their social media risk, but the most common reasons were a lack of resources to be able to accomplish the task.

Figure 3: Half of Companies Assess Their Risk

"Does your company currently assess its social media risk?"



Base: 39 of 61 respondents for whom social media risk management is their primary or a significant part of their responsibility.

Source: "Guarding the Social Gates: The Imperative for Social Media Risk Management," Altimeter Group (Aug. 9, 2012)

The Components of a Social Media Risk-Assessment Process

A social media risk assessment is a structured process for the objective evaluation and determination of the level of risk or exposure an organization faces specific to an identified threat or potential occurrence. Social media risk is composed of two primary components of likelihood and impact, and both of these components need to be examined within the context of an analytical methodology to be able to effectively assess the severity of a potential event (see Figure 4).

Figure 4: The Likelihood and Impact Components for Assessing Social Media Risk

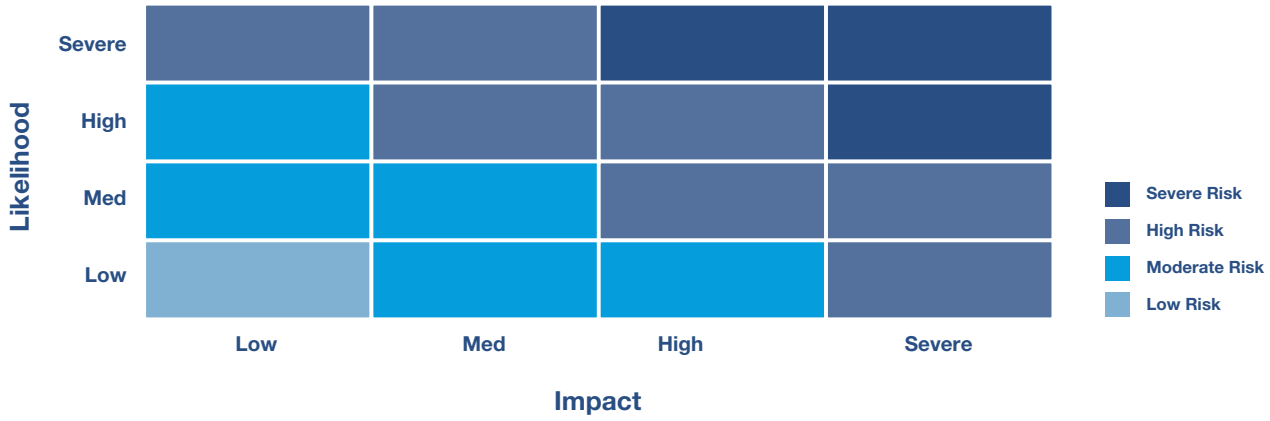
Component	Subcomponent
Likelihood. Likelihood is the first component of social media risk and is the probability of occurrence that something will happen.	**Catalyst.** Catalyst determines if there is a catalyst for action by the people or groups who would perpetuate the risk. It asks: Is there something that would cause people to act? Some social media risks have a definite catalyst for action, such as a product recall or a major news story. Other social media risks, such as the introduction of malware or reduced employee productivity, have much smaller and less well-defined catalysts. For example, a pro-environmental consumer might be motivated to sign petitions and write emails, but won't join a social media campaign against a large company until there is a catalyst for action.
	Opportunity. Opportunity asks: What is the breadth and depth of the opportunity of the channel? First, opportunity examines the accessibility of the channel — is this a public platform like Facebook, or is it walled off like an Enterprise Social Network? Second, social media is social, and one of the key aspects of social is the ability for something to go viral. Opportunity also examines what is the opportunity for this risk to perpetuate an increasing audience size.
	Motive. Motive looks at what is the underlying motivation for an actor. For example, a consumer who just wants to get their dishwasher fixed and feels like customer service won't listen to them is much different than an employee who accidently releases confidential information.
Impact. Impact is the second component of social media risk and refers to the expected effect or consequences (often negative) of an event or occurrence. Impact is commonly portrayed in the common denominator if financial loss.	**Reputation.** Reputation often means revenue, so this component looks at what would be the estimated impact due to the loss of reputation, primarily measured as the loss of current and future customers or sales. This could be reflected in loss of social media fans, significant shift in web traffic, a lower Net Promoter Score, or other measures.
	Availability. Availability looks at what would be the impact on the ability of the organization to service customers. For example, if social channels are your primary marketing channels, a lot of negative noise on that channel would lessen your marketing ability. Another example is a social customer service channel being inundated with negative comments instead of real customer service requests. This could make that channel unavailable to real customers.
	Legal/compliance. Legal, regulatory, and compliance risk is often a much more real and more tangible impact then many others, not just because of the potential financial damages, but because of the additional penalties and complications regulatory agencies and lawsuits can impose on a firm. For example, Lalit Modi, Chairman and Commissioner of professional cricket league Indian Premier League, had to pay more than $1.5 million in fines and legal fees after accusing another cricket player of match fixing on Twitter.

Source: "Guarding the Gates: The Imperative for Social Media Risk Management," Altimeter Group (Aug. 9, 2012)

The basic social media risk-assessment methodology used by some of the firms we spoke to is similar to many other risk-assessment methodologies. It focuses on understanding and estimating the likelihood of a threat event and the impact if the event occurs. From there, risks can be rated and resources applied against them to reduce likelihood and manage impact. The four steps are:

1. **Rate the likelihood that an individual event could happen.** The first component of this step is to rate what is the likelihood that an identified event will happen, with the scoring often based on experience. For some companies, this will be as simple as ranking each one either as a low, medium, or high likelihood. A more complex approach would be applying a quantitative rating based on a number of factors, such as a new product launch, recent attention in the news, or a targeting by an activist organization. For example, an organization may rate the likelihood of a brand reputation risk as a twice-a-month occurrence, but a legal risk may evolve rarely, once every two years.
2. **Rate the potential impact to the organization if it were to happen.** Again, based upon experience and an understanding of the organization and the market, determine what could happen. Be clear what the potential brand, market, financial, and customer impacts of the event could be. This could be as simple as ranking each potential event either as a low, medium, or high impact to as complex as applying a quantitative rating based on a number of factors of what the impact could be.
3. **Rank the risks.** Next, based upon the likelihood and potential impact of an event, rank the identified risk events. The most common approach is to place the scores on a matrix, with likelihood on the x-axis and impact on the y-axis according to scale or score, as in the example figure below (see Figure 5). For example, if Event A has a likelihood of High but only an impact of Low, it would be addressed under the moderate risk group. If two events are in the same risk group, the event with the higher likelihood should get ranked above the event with the higher impact. For example, if one event has a low likelihood and a severe impact, compared to an event with a high likelihood and a medium impact, the second event would get prioritized higher.
4. **Prioritize efforts and resources to manage and mitigate risk.** Based upon the ranking of the potential risk events, organizations should prioritize resources to either reduce the likelihood of the highest prioritized risk through implementation of additional controls and mitigation efforts or minimize the negative impact of such incidences.

Figure 5: Example of a Social Media Risk Matrix



Source: "Guarding the Social Gates: The Imperative for Social Media Risk Management," Altimeter Group (Aug. 9, 2012)

Step 3: Manage and Mitigate.

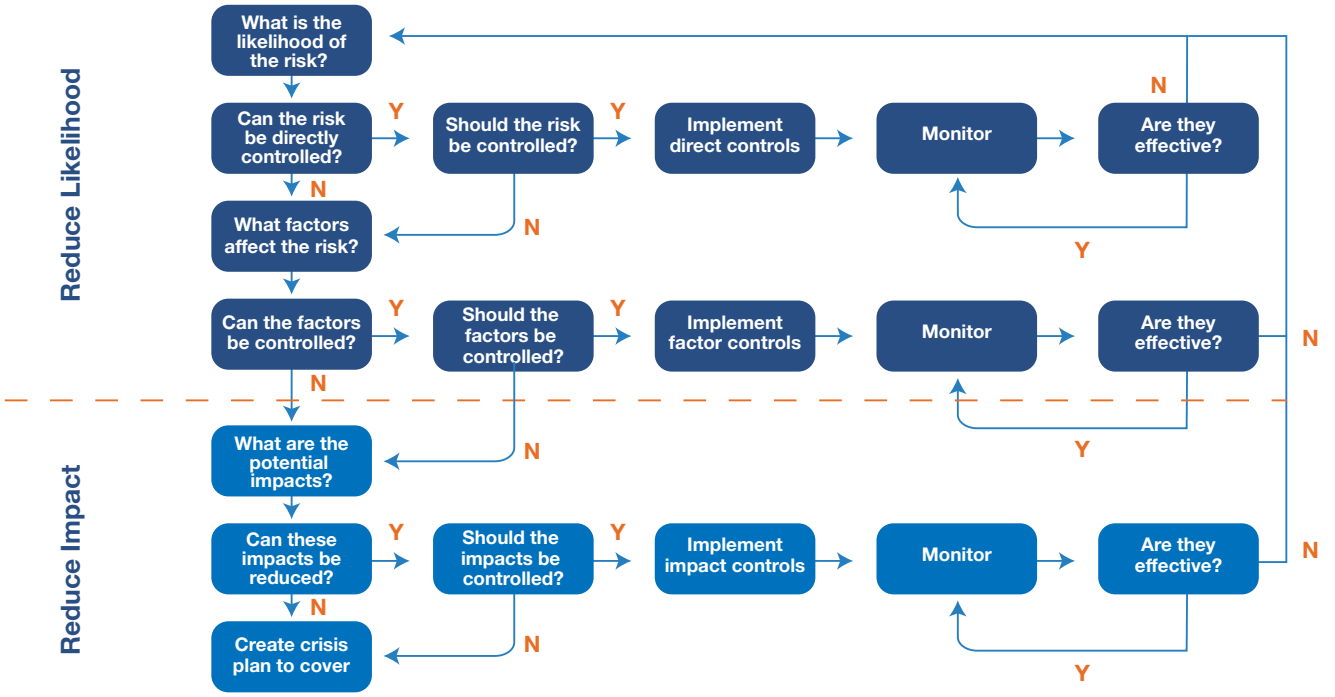
Once you have identified and assessed the risk, what are you going to do about it? Companies can manage and mitigate the risk through six steps:

1. Create a decision framework.
2. Put the right governance in place.
3. Staff with dedicated resources.
4. Protect the company and the employee with a set of policies.
5. Train employees on what the boundaries are.
6. Deploy appropriate tools.

1) Create a Decision Framework.

The first step is to use a risk control decision tree to systematically and thoroughly evaluate the controls against the risks based upon first reducing likelihood and then reducing the impact (see Figure 6). Reducing likelihood focuses on determining whether or not the risk can be directly controlled in the first place and then whether or not the factors that affect and perpetuate that risk can be mitigated. In contrast, reducing impact focuses on exactly that — making sure that the appropriate crisis control process is in place to minimize negative effects.

Figure 6: Example Process for Managing and Mitigating Risk



Source: "Guarding the Social Gates: The Imperative for Social Media Risk Management," Altimeter Group (Aug. 9, 2012)

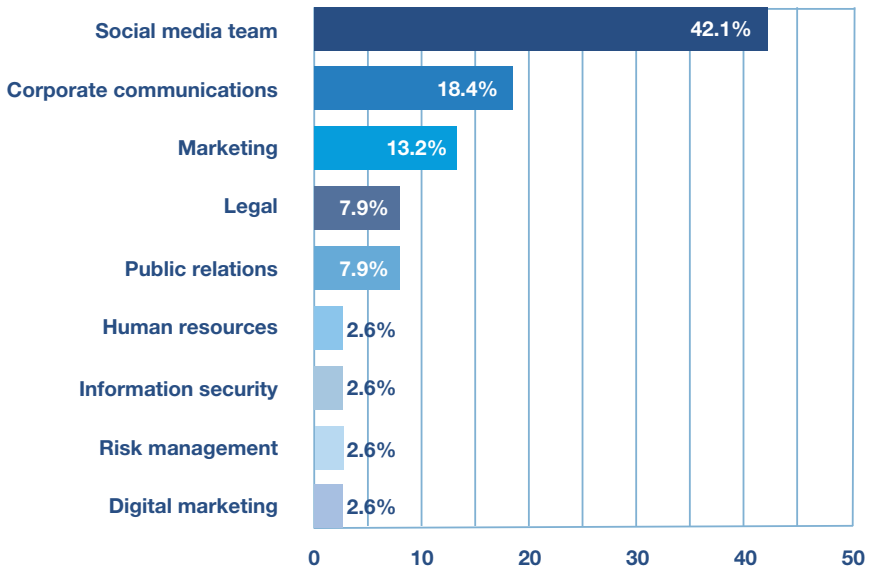
ALTIMETER

2) Put the Right Governance in Place.

The second component to good social media risk management is having the right roles and processes in place. In most organizations, but not all, the social media team is responsible for managing social media risk. We found that in approximately 50% of organizations we spoke with, the social media team is primarily responsible when it comes to social media risk management (see Figure 7).

Figure 7: Social Media Team is Frequently Tasked with Social Risk Management

"Which part(s) of the organization have a role in managing social media risk?"



Base: 39 of 61 respondents for whom social media risk management is their primary or a significant part of their responsibility.

Source: "Guarding the Social Gates: The Imperative for Social Media Risk Management," Altimeter Group (Aug. 9, 2012)

ALTIMETER

Even though the social media team is often the primary governance lead responsible for social media risk management, it shouldn't be the only department involved. One vendor we spoke with said that it has clients where social media risk management rolls up into legal, because of archiving and e-discovery issues, and from there up to the CFO. There are a number of possible configurations, because social media and social media risk affects a broad swath of any organization. From internal employee issues, such as training and monitoring handled by HR, to technology-based security issues handled by IT, a number of different groups and departments may have expertise that would assist in managing social media risk. One company we spoke with put it this way, saying, "HR, legal, and IT play the role of providing primary guidance on the infrastructure of what is needed behind all social programs."

Though every organization is different, Altimeter Group has identified six key organizational components that should to be involved in social media risk management (see Figure 8).

Figure 8: Six Key Organizational Components in Social Media Risk Management

Organizational Component	Role
Marketing	The marketing department is the department most often in charge of social media efforts, and, as such, plays a key role in overseeing the organizational social media brand presence. In most organizations, it is also responsible for social media risk management.
Human Resources	Human resources is critical to social media risk management, because it is often the group responsible for managing and monitoring the employee use of social media.
Legal and Compliance	Legal is generally responsible for laying down legal guidance on the appropriate use of social media. In regulated industries, compliance ensures that social media efforts are in compliance with the policies of the oversight agency.
IT and IS	IT and IS are responsible for internally hosted platforms, information security, and data loss prevention.
Communications and PR	Communications and PR are often responsible for organizational branding and crisis communications in the event of a crisis.
Security and Risk Management	Security and risk management are more traditional roles that are just beginning to get involved in social media risk management because of the role that social media plays in traditional physical and perimeter security (such as through social engineering).

Source: "Guarding the Gates: The Imperative for Social Media Risk Management," Altimeter Group (Aug. 9, 2012)

For example, one organization we spoke with has quarterly governance meetings of an established group that include representatives from marketing, corporate communications, legal, IT, and HR. Other organizations are more ad hoc in their approach. For example, one company had no specific structure for social media risk governance, but held weekly meetings between the social strategist and a representative from legal to ensure that what they were doing was within the policy bounds of the company.

3) Staff with Dedicated Resources.

Another key aspect is the amount of organizational resources that the company is willing to dedicate to the issue of social media risk management. Most companies have one to three employees who, as a part of their job duties, support the organization in addressing social media risk. In our *2012 Altimeter Social Media Risk Management Survey*, 43% of 39 companies we surveyed dedicate less than one FTE to social media risk management; and 31% had between one and five FTEs.

Some companies are taking social media risk more seriously and are staffing up. For example, both DuPont and Intel have one to two FTEs, including at least one person in a full-time social media risk management role identifying, assessing, and managing social media risk, in addition to other employees who support the social media risk management effort part-time.

To determine what resources are needed, emulate the steps that companies with more mature social media risk management processes have taken:

1. Identify the need for a resource for social media risk management based on the risk-assessment process outlined above.
2. Determine how much time is needed to manage the process based upon the risk assessment and current resourcing levels.
3. Determine what skill sets and technologies are necessary and what can be "outsourced" both within and outside the organization.
4. Hire, promote, or shift people to put the resource in place.

4) Protect the Company and Employee with a Set of Policies.

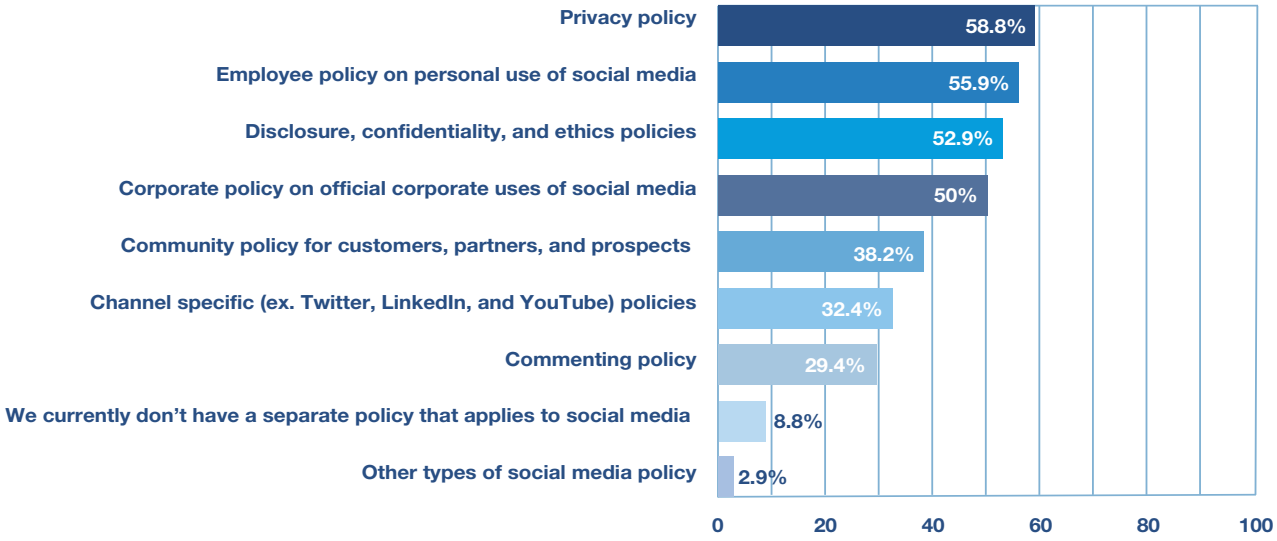
The fourth component to good social media risk management is having the right "fence lines" or policies in place.[12] Traditionally, social media policies, from a social risk-management perspective, primarily focused on one thing — minimizing the risk to the organization. But like many other things, minimizing that risk has a tradeoff. If organizations try to minimize the risk too much, they do so at the expense of the primary purpose of social media — being social. Policies need to define what should not be done, and then, when you do engage, how to do so in a way that minimizes risk.

When it comes to existing social media policies at companies, the most common type of policy is a privacy policy (see Figure 9.1), with 59% of 34 companies we surveyed in our *2012 Altimeter Social Media Risk Management Survey* reporting that they had a privacy policy in place. These privacy policies commonly build on the digital privacy policies that were put in place for interactions through websites and email. Other social media policies that most companies have include an employee policy on the personal use of social media (56%); disclosure, confidentiality, and ethics policies (53%); and a corporate policy on the corporate use of social media (50%).

When a company does have a social media policy, we found that most of these policies are updated less than annually (see Figure 9.2). A best practice exposed by some of the companies that we spoke to is that a social media policy should be reviewed and updated twice a year to match the pace of technology change.

Figure 9.1: Privacy Policy is the Most Common Social Media Policy

"Which of the following social media policies or other policies that either include social media or are referenced back to in social media policies does your company currently have?"

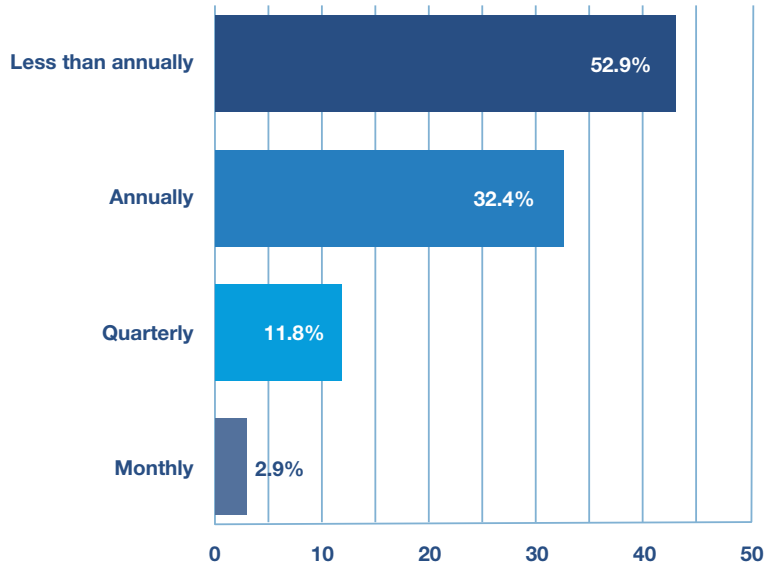


Base: 34 of 61 respondents for whom social media risk management is their primary or a significant part of their responsibility.

Source: "Guarding the Social Gates: The Imperative for Social Media Risk Management," Altimeter Group (Aug. 9, 2012)

Figure 9.2: Social Media Policies Are Not Updated Frequently

"How often are these policies updated?"



Base: 34 of 61 respondents for whom social media risk management is their primary or a significant part of their responsibility.

Source: "Guarding the Social Gates: The Imperative for Social Media Risk Management," Altimeter Group (Aug. 9, 2012)

Though there are multiple types of social media policies, most policies fit into three categories (see Figure 9.3). These categories can and should overlap in their application. A good social media policy is a balance point between minimizing risk to the organization and shared responsibility between the organization and others.

Figure 9.3: Three Primary Social Media Policy Categories

Category	Explanation	Example Policy Types
Participation	Social media participation policies outline at a tactical level how people and groups participate (or don't participate) in both formal and informal communities.	**Privacy:** Determine how the organization will use the information it gathers as it participates.
		Employee participation: Document which employees are allowed to participate in social media on behalf of the organization and what they should and shouldn't do.
		Community: Detail the common objectives of a formal community, who is allowed to participate in a formal community, and the boundaries for participation within that community.
Ethics	Ethics policies cover at a strategic level what is right and wrong behavior in social media.	**Disclosure:** Outline what information is okay to release, what isn't, and under what circumstances.
		Code of conduct: Document what is the appropriate desired behavior of both employees and customers, both personally and professionally.
Operational	Operational policies cover the risk and execution of the aspects beyond social media.	**Organizational purposes for social media:** This policy outlines the strategic purposes of why an organization chooses to participate in social media and what employees, customers, and partners can expect from the organization.
		Information security: Outline the different security precautions to take with social media.

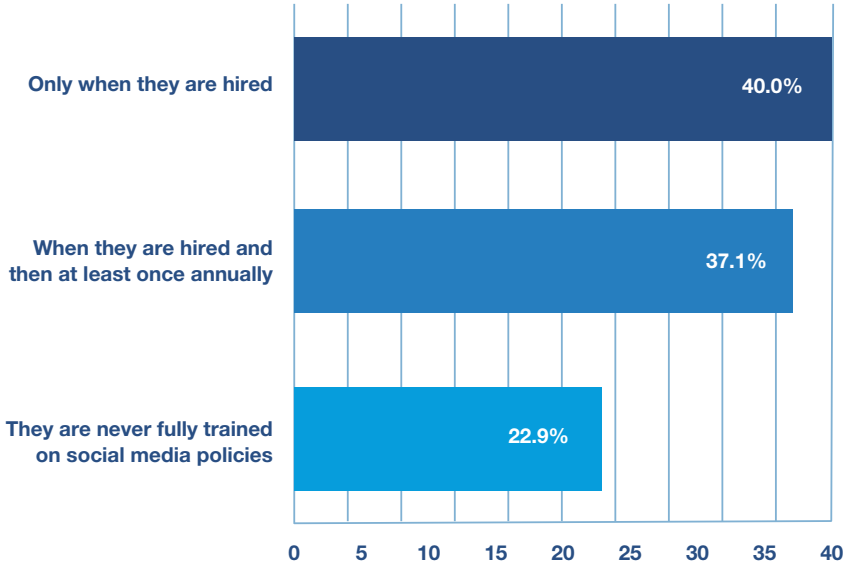
Source: "Guarding the Gates: The Imperative for Social Media Risk Management," Altimeter Group (Aug. 9, 2012)

5) Train Employees on What the Boundaries Are.

If you have social media risk governance established, have the right kinds of policies and covenants in place, and have a process for updating them on a regular or as-needed basis, the next step is making sure employees and executives are appropriately and regularly trained. Altimeter Group found that approximately 60% of 35 companies we surveyed in our *2012 Altimeter Social Media Risk Management Survey* never train employees about social media or only when they are hired (see Figure 10). Given the constant state of change of social media and the risk that social media has for the organization, employees should be given annual training on organizational social media policies and processes. This can be integrated into existing training on privacy or compliance training or a course with a dedicated focus.

Figure 10: Training on Social Media Policies is Lacking

"How often are employees trained on the social media policies commonly?"



Base: 35 of 61 respondents for whom social media risk management is their primary or a significant part of their responsibility.

Source: "Guarding the Social Gates: The Imperative for Social Media Risk Management," Altimeter Group (Aug. 9, 2012)

6) Deploy Appropriate Tools.

Last but not least, having the right technologies in place to support and scale social media risk management is essential. The bad news: There aren't a lot of technology tools that are currently designed and dedicated for social media risk management. Most tools used in social media risk management are multi-purpose tools or tools that have been appropriated from other purposes. There are three general tool categories in this fledgling space: 1) monitoring and listening tools, 2) social media management systems, and 3) social media compliance systems (see Figure 11).

Figure 11: Key Social Media Risk Management Tool Categories

Category	Overview	Tools
Monitoring and Listening	Social media monitoring and listening platforms are the same tools that organizations use to listen to what their customers are saying in the social space. In social risk management, they are also used for nearly the same purpose, turned toward listening for risk-indicating statements from customers and leakage of internal information by partners and employees.	Options range from simple tools, like Google alerts and Facebook searches, to more advanced listening tools, like Salesforce Radian6 and Crimson Hexagon, to full-on analytics packages, like SAS.
Social Media Management	Social media management tools are tools that organizations use to organize, manage, and automate their social media workflow, including publishing. From a social media risk management perspective, some of these same tools can also be used to manage and control what information is released by the organization. For example, some tools can scan outgoing corporate social messaging and flag inappropriate content or content in violation of corporate guidelines. This would be especially important for companies operating in a highly regulated environment.	This category includes a broad set of tools and technologies, like Actiance, Awareness, Expion, Hearsay Social, Inc., Hootsuite, Social iQ Networks, Sprinklr, SproutSocial, Syncapse, and others.
Social Media Compliance	Social media compliance tools are functionalities and tools that assist organizations in complying with either internal policies and/or external regulatory requirements. These tools enable activities such as archiving of social media activity, auditing social media activity, and monitoring employee social activity.	This category of tools includes Actiance, Jive, Kronovia, Smarsh, Social iQ Networks, SocialLogix, Socialware, and others.

Source: "Guarding the Gates: The Imperative for Social Media Risk Management," Altimeter Group (Aug. 9, 2012)

Step 4: Monitor and Evaluate.

Social media is and will remain a dynamic, constantly shifting space for the foreseeable future. So the risk identification, assessment, and mitigation efforts you did last week, last month, and last year won't be entirely applicable to the risks you face today or tomorrow. Your social media risk management efforts will need to continue to evolve against the changing threats. To do that, focus on continuously monitoring and assessing evolving threats and evaluating the mitigation and control efforts against the threats.

Risk assessments and mitigation efforts should be reviewed on a regular (every six months to annually) basis to ensure that there continues to be coordination between assessments and mitigation efforts. For example, one company we spoke to runs a monthly session that looks at current risks, emerging risks, and the effectiveness of mitigation and control efforts.

In addition to these regular reviews, risk assessments and mitigation strategies should be reviewed or updated under the following circumstances:

- **Entering a new channel.** Whenever an organization is making the determination to enter a new social channel or platform, a risk assessment should be done along with an examination of the ability of current mitigation and control mechanisms to handle any additional risks identified in this new channel. For example, a financial services firm we spoke to did an extensive social media risk assessment before launching a social media-based customer service channel.
- **Solid emergence of a new technology.** Whenever a new technology begins to solidly emerge with broad adoption, an evaluation should be done to ensure that the risk assessment is up to date and that the mitigation and control efforts cover this new technology. For example, one company we spoke to said that once a social media platform reaches 50 million potential customers, such as Google+ did, it begins to include it in its risk assessment. Even if the company is not planning on embracing a new technology, what should drive the risk assessment is the channel or platform adoption (either actual or potential) by the organization's customers.
- **Identification of a new threat.** If a new threat emerges, then the risk assessment needs to be checked against the new threat to ensure that the appropriate control and mitigation strategies are in place.

Next Actions: Get Your Organization's Head Out of the Sand

Good social media risk management practices are your insurance that you will be prepared to address, mitigate, and manage social media risks to keep them from turning into social media crises. To ensure the odds of success of your nascent risk management process, do the following:

- **Make social media risk a board issue.** The primary reason that there is a continuing growth in social media crises and social media contributing to other crises is because most company leaders don't perceive social media as a risk, in much the same way that most executives and boards didn't perceive the internet as a risk until the first malware showed up. Be proactive in making social media risk a board-level issue, given its potential to significantly impact the value of the company. For example, IBM makes social media risk a board-level issue.[14]

  While some of the day-to-day tasks can be delegated down, executives need to be involved in the decision-making and oversight. Build awareness of this responsibility by educating key leaders (up to and including board of directors) that social media has both an upside and a downside and that they need to be aware of — and engaged in — understanding both.

- **Learn from past crises.** Whether it is within your organization or another, there is a new social media crisis every week, and these crises often provide great potential case studies on what to do and what not to do when it comes to social media risk management. Pick a crisis, do some background research to better learn what led up to that crisis and how the organization responded, and then war-game out the crisis as if it happened to your organization. Begin by asking: How would your organization have responded differently? How would your organization have responded the same? What processes, tools, and policies would have helped? And if this would have happened anyway, how could you minimize the impact?

- **Review your own responses.** Most organizations we interviewed said that they faced one or two significant social media crises on an annual basis. These events provided a great learning laboratory after they were over. After dealing with a potential or actual social media crisis event, run post-mortem reviews by asking and answering the following questions:
  - What actually happened?
  - What were the primary factors leading up to the event?
  - Which of those factors could we influence?
  - Which of those factors could we control?
  - Was this event predictable? If so, did we predict it? If we didn't predict it, why not?
  - What worked in mitigating the risk? What didn't?
  - What do we need to change now?

- **Test through scenario exercises.** The only way to know if the social media risk management effort your organization has put in place will work is to test it. One of the best ways to test it is by running scenario exercises or war-gaming different risk scenarios. These should be done on a regular basis (every quarter to an annual basis) and involve different levels and departments around the organization. For example, a basic exercise may involve the ability of the listening team to find and recognize different risks. A more complicated and extensive exercise would involve running the whole social media management effort all the way up to the CEO through a multi-faceted social media risk management and crisis exercise.

Ecosystem Input

This report includes input from market influencers and solutions vendors who were interviewed or briefed by Altimeter Group during the course of this research. Input into this document does not represent a complete endorsement of the report by the companies listed below.

Brands (17)

AAA, Kim Snedaker, Social Media Strategist AAA Club Partners
Cisco, Lasandra Brill, Senior Manager Global Social Media
Dell, Liz Bullock, Director Social Media & Community
Dell, Ryan M. Garcia, Legal Director Social Media
Dell, Richard Margetic, Director Global Social Media
DuPont, Heather Read, Social Media Issues & Crisis
DuPont, Gary Spangler, Corporate eMarketing Manager at DuPont
IBM, Gadi Ben-Yehuda, Social Media Director for The Center for the Business of Government
Intel, Rick Reed, Issue & Crisis Manager
Red Cross of America, Wendy Harman, Social Media Director
The Weather Channel, Renee Willet, Manager Social Media Marketing
Toyota, Florence Drakton, Social Media Manager
Toyota, Kimberley Gardiner, National Digital Marketing & Social Media Manager
WellPoint, Jonathan Blank, Manager of Social Media
Wells Fargo, Ed Terpening, Vice President Social Media

Note: Two brands are not listed for confidentiality reasons.

Professional Services and Agencies (12)

247 Laundry Service, Jason Stein, Founder & President
Big Fuel, Michoel Ogince, Director, Platform and Product Strategy
C7group, Jeff Marmins, CEO and Founder
Edelman, Michael Brito, SVP Social Business
Grant Thornton LLP, Lucino Sotelo, Head of Digital Marketing
Grant Thornton LLP, Jan Hertzberg, Managing Director Business Advisory Services
Hill+Knowlton Strategies, Andrew Bleeker, Worldwide Director of Digital
Ketchum, Jonathan Kopp, Partner and Global Director
KPMG, Sanjaya Krishna, Digital Risk Consulting Leader
KPMG, H. John Hair, Director KPMG Advisory Services
PricewaterhouseCoopers LLP, Jack Teuber, Managing Director Online Marketing
Weber Shandwick, David Krejci, Executive Vice President Social Media and Digital Communications

Vendors (13)

Actiance
Crimson Hexagon
Hearsay Social, Inc.
Kronovia
rPost
RSA (EMC)
Salesforce Radian6
SAS
Secure.me
Smarsh
Social iQ Networks
SocialLogix
Socialware

Acknowledgements

With thanks for support from: Regina Denman, Asha Hossain, Cheryl Knight, Christine Tran, and Alec Wagner.

End Notes

[1] A research survey by InSites Consulting of more than 1,200 global company managers, found that eight out of ten American companies are present on Facebook, 45% have a twitter account, 48% are on LinkedIn, and 31% are on YouTube. Please see "Survey Shows 80% of Companies Use Facebook," Vending Market Watch, June 20, 2012; www.vendingmarketwatch.com/news/10732362/survey-shows-80-percent-of-companies-use-facebook. Retrieved on June 22, 2012.

[2] According to the IBM 2012 Global CEO Study of 1,709 CEOs interviewed, 16% of their companies use social platforms to engage with their customers, with that number expected to jump to 57% within a period of three to five years. Please see Leading Through Connection: 2012 Global Chief Executive Study, IBM Institute for Business Value; www.ibm.com/ceostudy2012/. Retrieved June 22, 2012.

[3] With most organizations, the primary social risk is not participating in the social space. Even the most heavily regulated and conservative organizations have come to understand that whether or not they choose to participate, there are already conversations taking place about the organization and that it is better to be a part of those conversations then not.

[4] Other areas pose just as great a risk, but they are more relevant to certain industries, platform adoption, or customer base. For example, one company that does a lot of government and financial services work reported that a deep investigation of the background of a person who was trying to connect with all of the key members of a project via LinkedIn actually had multiple different personas and had originated from an Asian country. Essentially, they were using a social channel for social engineering to attempt to penetrate the company.

[5] It is unusual to see executives make social media mistakes, but it can happen. Please see "Facebook and Twitter Postings Cost CFO His Job," The Wall Street Journal, May 15, 2012; http://online.wsj.com/article/SB10001424052702303505504577404542168061590.html. Retrieved July 23, 2012.

[6] Allergy Pathways was sued by the Australian Competition & Consumer Commission after fans posted misleading positive comments about its products online on Facebook, Twitter, and other social channels. Even though Allergy Pathways didn't write the posts, since it should have known they were misleading and instead left them up on the sites, according to the court, it then became the publisher and was responsible. See the findings from the ACC at www.accc.gov.au/content/index.phtml/itemId/972417/fromItemId/142.

[7] Brands being attacked and hijacked by activist organizations, like Greenpeace and others, is becoming more common. Please see Asher Moses article "Shell Social Media Oil Spill a 'Coordinated Online Assassination'" in the Sydney Morning Herald, July 19, 2012; www.smh.com.au/technology/technology-news/shell-social-media-oil-spill-a-coordinated-online-assassination-20120719-22bpe.html. Retrieved July 26, 2012.

[8] In 2009, Mommy Blogger Heather Armstrong (aka Dooce) called Whirlpool customer service over Whirlpool's inability to fix her almost-new Maytag (a subsidiary of Whirlpool) washing machine. When she wasn't able to get what she felt was an appropriate and helpful response from the rep or their supervisor, she resorted to what amounts to a veiled threat — asking the customer service rep if Whirlpool knew what Twitter was and that she had over a million followers. Whirlpool's response? Essentially, "So what?" And, with that, Whirlpool missed an opportunity to identify and respond to a potential risk to its brand that could have been alleviated through good customer service.

[9] The issue with the share widget was that it didn't give consumers full information, only sharing the positive aspects about the drug and not the associated risks. Please see Mike Masnick's article "FDA Tells Novartis That 'Facebook Sharing' Widget on its Site Violates Drug Ad Rules," TechDirt, August 10, 2010; www.techdirt.com/articles/20100806/15182710535.shtml. Retrieved July 24, 2012.

[10] Dr. Tran's transgression was not necessarily in that she was posting about her experiences on Facebook, but that she was giving away enough information that patients could be identified. See www.msnbc.msn.com/id/42652527/ns/technology_and_science-security/t/doctor-busted-patient-info-spill-facebook/#.UBQatDGe7Sw.

[11] The Intel Threat Agent Library is a compilation of threat agent personas that Intel and other companies can then defend against. According to the Intel site, Intel IT Threat Assessment Group developed to drive a standardized reference to human threat agents that pose threats to IT systems and other information assets. See the site and the library at http://communities.intel.com/docs/DOC-1151.

[12] Altimeter Group Founder Charlene Li lays out the different types of social media policies, the importance of accountability, and more in her book Open Leadership. Please see Charlene Li, Open Leadership, Jossey Bass, 2010.

[13] For a deeper look at different social media management systems and how to manage proliferation of platforms, see Jeremiah Owyang's A Strategy for Managing Social Media Proliferation, January 5, 2012. www.slideshare.net/jeremiah_owyang/smms-report-010412finaldraft

[14] IBM CMO Jon Iwata shared that social media risks are regularly reviewed at IBM board meetings, at the IBM CMO CIO Leadership Exchange 2012, June 6, 2012.

Open Research

This independent research report was 100% funded by Altimeter Group. This report is published under the principle of Open Research and is intended to advance the industry at no cost. This report is intended for you to read, utilize, and share with others; if you do so, please provide attribution to Altimeter Group.

Permissions

Disclosures

Your trust is important to us, and as such, we believe in being open and transparent about our financial relationships. With permission, we publish a list of our client base on our website. See our website to learn more: www.altimetergroup.com/disclosure.

Disclaimer

About Us

Alan Webber, Altimeter Partner, Analyst

Alan Webber (@alanwebber) is an Industry Analyst and currently the Managing Partner at Altimeter Group. Alan's research and client efforts focus on the understanding and thriving through disruptions at intersection of organization, culture, and technology. Alan publishes some his findings on his professional blog www.RoninResearch.org. Prior to Altimeter, he was a Principal Analyst at Forrester Research where he covered the B2B online user experience, digital engagement, and disruptive technologies in government.

Charlene Li, Altimeter Founder and Partner, Analyst

Charlene Li (@charleneli) is Founder of the Altimeter Group and the author of the *New York Times* bestseller, *Open Leadership*. She is also the coauthor of the critically acclaimed, bestselling book *Groundswell*, which was named one of the best business books in 2008. She is one of the foremost experts on social media and technologies and a consultant and independent thought leader on leadership, strategy, social technologies, interactive media, and marketing.

Jaimy Szymanski, Researcher

Jaimy Szymanski (@jaimy_marie) is a Researcher with Altimeter Group where she researches and analyzes how organizations can effectively utilize social media and other disruptive technologies to achieve business advantage. She has experience working in business consulting, content marketing, and social media research and advisory roles.

Altimeter Group is a research-based advisory firm that helps companies and industries leverage disruption to their advantage.

Contact Us

Altimeter Group
1875 S. Grant Street, Suite 680
San Mateo, CA 94402-2667
info@altimetergroup.com
www.altimetergroup.com

Advisory Opportunities

Email: sales@altimetergroup.com