WHITE PAPER

# Mapping Organisational Roles & Responsibilities for Social Media Risk

A Hootsuite & Nexgate White Paper

Hootsuite™

NEXGATE

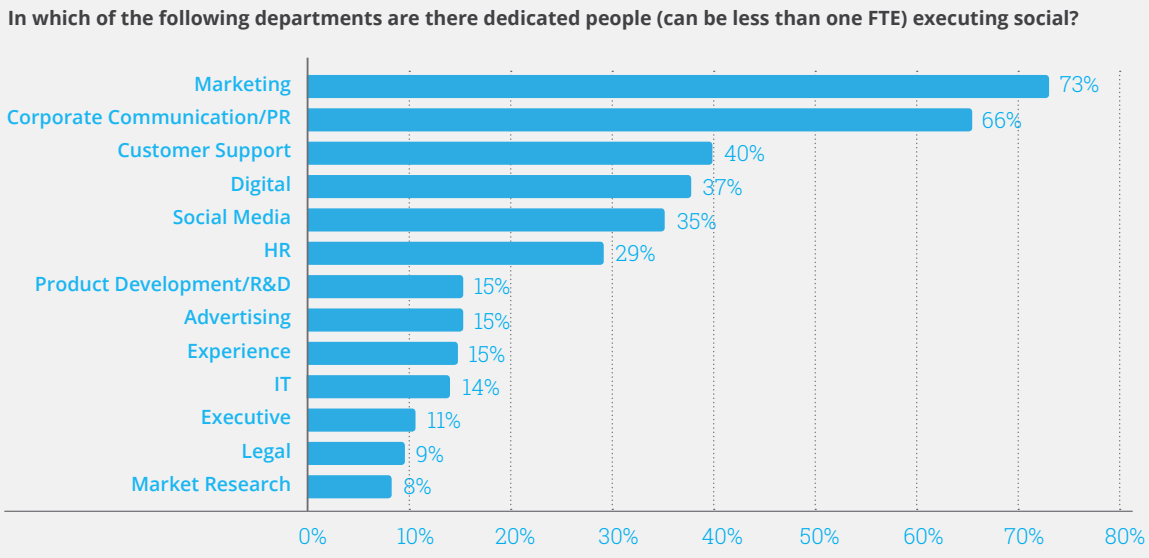
# Mapping Organisational Roles & Responsibilities for Social Media Risk

## Executive Summary

Social media has introduced a wide array of opportunities for organisations to engage with customers, employees, and partners. Marketing, customer service, and a variety of other business functions are now capitalising on these opportunities, using new tactics and tools. But with these opportunities come risks: damaged brand reputation, regulatory violations, privacy issues, intellectual property compromises, phishing, malware, and more. What is less clear is who is responsible for managing and mitigating the risks tied to social media.

To get optimal value from social media efforts, organisations need to establish controls for the potential downsides of the technology. Every enterprise must begin by clearly defining which roles within its unique corporate structure should be involved in social media risk management and the specific responsibilities of each role. Those roles then need to be given the policies and technologies they require to be successful at identifying, managing, and mitigating social media risks. This report will outline a framework for assigning roles and responsibilities and explain how enterprises can prepare themselves for real-world risk scenarios.

Figure 1: Thirteen Departments Are Actively Engaged in Social Media




*Base: 125 respondents with companies of 1000+ employees*
*Source: Altimeter Group Social Business Strategy Survey, Q4, 2012, "Social Data Intelligence," Altimeter Group (July 25, 2013)*

# Roles With an Interest in Social Media Risk Management

More than just another marketing channel, social media is a fundamentally new form of communication which is seeing adoption in almost every functional area of the modern enterprise. The ubiquity of social media prompts the question: who is responsible for managing the risks? While it's obvious that the CIO is responsible for managing IT risks, such as hackings and hardware downtime, and the CFO is responsible for managing financial risks, such as regulatory changes and fraud, the answer is less clear for social media.

With the unique nature of social media, responsibility for managing and mitigating social media risk is often spread across a number of corporate functions, including Marketing, IT, Communications, Legal, Audit, Risk, and Human Resources.

The best way for companies to align organisational responsibility is to break it down by three levels — titles, roles, and responsibilities — across seven necessary functional areas:

**Marketing and Communications Management**

- **Representative Titles:** Chief Marketing Officer, Vice President of Marketing, and Vice President of Corporate Communications.
- **Role Level:** Strategic.
- **Social Media Responsibilities:** Generally serves as executive sponsor or executive owner of social media initiatives within an overall marketing and brand management effort. Accountable to the Board of Directors and executive team for the success and failure of social media efforts, including social media activity and brand presence, return on investment, and any associated crises.
- **Key Social Media Risk Concerns:** Brand and image protection, reputation management, and regulatory compliance for Marketing.

**Information Technology**

- **Representative Titles:** Chief Information Officer and Chief Information Security Officer.
- **Role Level:** Strategic.
- **Social Media Responsibilities:** Generally serves as executive co-sponsor or co-owner of social media initiatives and efforts within the context of an overall information technology architecture and an overall security architecture. Accountable to the Board of Directors and Chief Executive, in conjunction with the CMO, for social media compliance, privacy, IP and company information protection, and any channel breaches.
- **Key Social Media Risk Concerns:** Regulatory compliance, data privacy and security, social engineering, data management, and network and resource protection.

**Social Media Technology**

- **Representative Titles:** Chief Technology Officer, Enterprise Architect, Digital Security Manager, and Digital Infrastructure Manager.
- **Role Level:** Strategic to tactical.
- **Social Media Responsibilities:** Select, deploy, and standardise social media management applications and tools, social media account management, social media policy enforcement, and social media training.
- **Key Social Media Risk Concerns:** Social media account security, social media privacy, API vulnerabilities, standardisation of risk mitigation efforts across channels, app proliferation, and channel proliferation.

**Social Media Marketing**

- **Representative Titles:** Director/Manager of Social Media, Director/Manager of Digital Marketing, Director/Manager of Corporate Communications, and any agencies with social media responsibility.
- **Role Level:** Managerial.
- **Social Media Responsibilities:** Responsible for day-to-day management of social media efforts including channel management, content and channel planning, content creation and approval, channel and application security, social analytics, social network monitoring, and initial issue and crisis identification and response.
- **Key Social Media Risk Concerns:** Internal and external (fraudulent or copycat) channel and site proliferation, minimising operational risks through policies and training, and on-channel security management.

**Social Community Management and Customer Service**

- **Representative Titles:** Social Community Manager and Social Customer Service Manager.
- **Role Level:** Managerial and operational.
- **Social Media Responsibilities:** Day-to-day customer interaction, community management, monitoring of the community and brand in the social landscape, and management of acceptable-use policies.
- **Key Social Media Risk Concerns:** Poor community management, inappropriate community use, customer interactions, customer data management, social media spam, and customer issue escalation and intensification.

**Legal and Audit**

- **Representative Titles:** Chief Legal Officer, Chief Compliance Officer, Chief Risk Officer, Compliance Manager, and Audit Manager.
- **Role Level:** Strategic to operational.
- **Social Media Responsibilities:** Regulatory and legal compliance, oversight of social media policies and governance, auditing of brand accounts, fraud identification and management, ensuring standardization of the brand and brand compliance across social networks, identification and addressing of brand hijacking, and brand/reputation management and protection.
- **Key Social Media Risk Concerns:** Brand compliance, including internal use, partner and affiliate use, and community use, intentional and unintentional brand hijacking, and erosion of brand reputation.

**Human Resources**

- **Representative Titles:** Chief People Officer and Director/Manager of Human Resources.
- **Role Level:** Strategic to operational.
- **Social Media Responsibilities:** Employee oversight, training on social media governance, policies and tools, and management of internal non-compliance with social media policies.
- **Key Social Media Risk Concerns:** Lack of employee training on social media policies and tools, identification and correction of employee actions on social media, and safety of employee personal use of social media.

# Planning a Social Media Risk Management Strategy

For too many companies, initial social media efforts are haphazard and uncoordinated, yet require the participation of multiple departments. Marketing has set up a Facebook page and maybe a Twitter feed, Human Resources has established a presence on LinkedIn for recruiting, individual sales reps are tweeting away, and IT is trying to lock down all of the systems to protect the company. This lack of strategic alignment not only exposes the organisation to unnecessary risk, but greatly restricts the business potential of its social media efforts.

Every enterprise requires a corporate strategy for social media, with risk management as one of its cornerstones. An executive sponsor from Marketing or Corporate Communications is often critical in gaining strategic alignment, but stakeholders from across the organisation should be involved in the process. Effective social media risk management requires internal coordination across departments and groups for the following:

1. Agreeing on the corporate purposes and strategy for adopting social media channels and platforms;
2. Claiming the corporate geography on the different social media channels;
3. Monitoring access, content, and applications across the social landscape;
4. Putting together and executing an implementation plan for the strategy, including a crisis communications and response plan; and
5. Following up on the execution, including success metrics.

None of these responsibilities can be fulfilled without help from multiple parts of the organisation. Though different for each enterprise, effective social media risk management requires the active participation of, at the minimum, Marketing, IT, and Legal, and perhaps other departments such as Human Resources, Audit, and Customer Service.

**Roles and Responsibilities in Common Risk Scenarios**

Once roles with a vested interest in social media risk management are identified, clear lines of responsibility need to be defined. The best way to do this is to recognise common risk scenarios that the company faces from social media and to establish the responsibilities of involved departments and groups in addressing those scenarios.

Below are five common risk scenarios and issues in social media. For each one, a high-level overview is provided, along with example roles and responsibilities found in most organisations.

## Scenario 1: Tracking and reporting approved and fraudulent social media accounts

**Overview:** It is determined that someone external to the organisation has set up one or more unauthorised social media accounts that purport to represent the organisation.

**Roles and Responsibilities:**

- Social Marketing tech team and any agency supported and services, Marketing, and IT are responsible for monitoring for new, unauthorised accounts.
- Legal is responsible for notifying the social network with a request to remove the account. Once complete, Legal should report back to Marketing for verification.

## Scenario 2: Social media account being hacked

**Overview:** One or more social media accounts are compromised and unauthorised content is published on those accounts.

**Roles and responsibilities:**

- Corporate Communications is responsible for having a defined (and tested) internal/external communications plan and process created that includes agency support.
- Social Media with any agency support is responsible for monitoring all social channels.
- Marketing leads communications with the advisement of Legal.
- IT leads from a systems perspective, interfacing with Marketing and the social networks.
- IT Security should investigate and respond to each incident as a security breach, and take actions to preclude future risk.
- Marketing and Security should report to a broader Social Media Committee and Board with regard to outcome and risk mitigation.

## Scenario 3: Spam and malware content identified

**Overview:** Malware, and to a lesser degree spam, is identified either being introduced through or existing on corporate social media accounts.

**Roles and responsibilities:**

- Community Manager first identifies the bad content, ideally using automated technology, implemented with the support of IT Security and policy already defined by Legal.
- Security and Legal review incident reports, remediation efforts, and workflow periodically for verification.

## Scenario 4: Release of customer data

**Overview:** There is the potential for a release of customer data either by the customer, inadvertently by the company, or through hacking efforts.

**Roles and responsibilities:**

- Community Manager should identify incidents using technology configured by the IT security team, under the guidance of Legal and/or Compliance.
- Community manager and Social Media team should audit and report issues regularly to Legal and/or Compliance.
- Legal and/or Compliance should monitor incidents and changes to laws and government guidelines, and recommend necessary policy changes accordingly.
- Risk Management should evaluate risk to the organisation based on the potential, volume, and severity of incidents.
- Compliance reviews incidents and handling of regulated or controlled data in coordination with IT Security.

## Scenario 5: Compliance violations or release of sensitive company data

**Overview:** The company has the potential for violations of compliance regulations or is susceptible to unauthorised release of company data.

**Roles and responsibilities:**

- Legal and/or Compliance should define a policy and plan for addressing this issue, based on state, regional, and industry requirements.
- Legal and/or Compliance should work with the Social Media team to understand application, and with IT to map technology against enforcement capabilities.
- Compliance reviews incidents and handling of regulated data, and adjusts policy and rules for communication on a regular basis.
- IT Security implements the policy via technology controls.
- Social Media team follows defined process and is audited, and reports back on progress and any irregularities or challenges to the workflow.

## Who is Responsible for the Costs?

After determining who is responsible for the various aspects of social media risk management, an organisation must answer the question, "Who pays for it?"

The actual technology cost for a risk and compliance solution or monitoring application is usually shared between IT and Marketing or Corporate Communications.

Other costs, such as legal, audit and compliance support, are often taken on by other groups in whole or with a chargeback mechanism to Marketing. The cost of training all employees on good social media policies and practices is often covered by Human Resources or treated as a general corporate expense; however, individual departments may allocate portions of their budgets to training specific groups such as Customer Service Representatives.

**Figure 2: Functional Areas and Common Social Media Risk Cost Responsibilities**

| | |
|---|---|
| Marketing & Communications Management | • Agency services and support fees (Marketing)<br>• Social media risk management system (Share with IT)<br>• Social media listening system (Share with IT)<br>• Other social media technologies and platforms (Share with IT) |
| Information Technology | • Social media risk management system (Share with Marketing and Communications)<br>• Social media listening system (Share with Marketing and Communications)<br>• Other social media technologies and platforms (Share with Marketing and Communications) |
| Social Media Technology | • Ongoing management of social media risk management system<br>• Ongoing management of social listening system |
| Social Media Marketing | • Staffing costs of social media marketing efforts, including agency services |
| Social Community Management & Customer Service | • Staffing and related costs of community platforms and social customer management systems |
| Legal & Audit | • Staffing and related costs related to legal management and ongoing audit efforts |
| Human Resources | • Staffing and related costs related to social media training<br>• Staffing and related costs related to internal policy management |

# Making It Real: Actual Responses to Social Media Risk

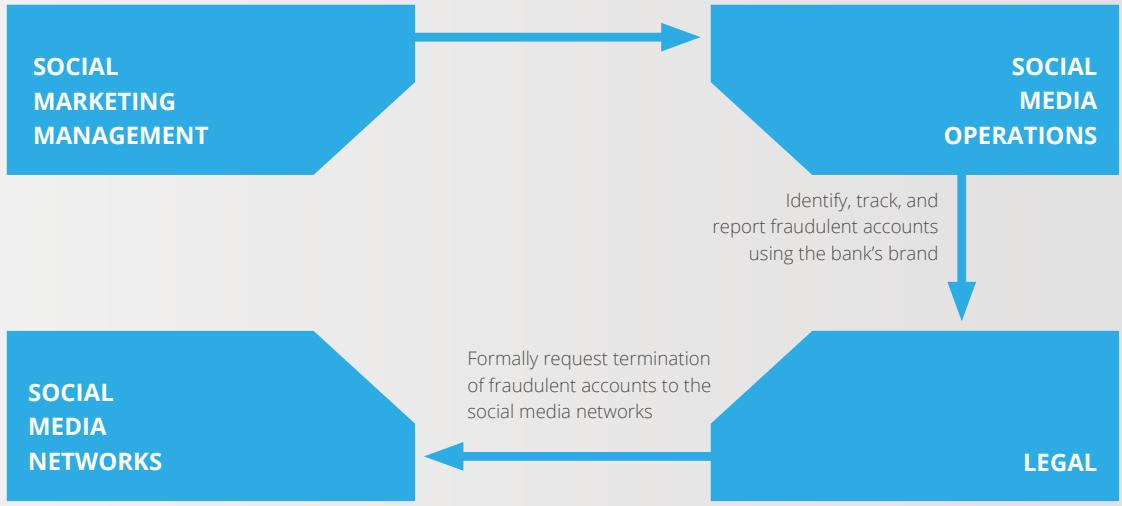
In order to understand how social media risk management plays out in reality, we spoke with the former Vice President of Social Media for one of the world's largest financial institutions. He described two real-world cases, and how his cross-functional team worked together to manage them.

## Case One: Discovering and tracking bank-owned social media accounts and reporting fraudulent accounts

At our bank we had a Social Media Operations team that reported to me as the head of Social Media. The staff on the operations team was responsible for finding, via any mechanism possible, social accounts owned and being run by the bank. This involved web searches, as well as querying the social networks via their native search tools, and leveraging data from listening platforms.

The team maintained a running list of accounts. For any accounts that were deemed "unauthorised," we would try to connect directly via internal company communications to either authorise and incorporate the account, or have it shut down. For any accounts that were external and were found to be fraudulent and otherwise inappropriately using our bank's brand, we would report the account to our assigned legal resource. The Legal Compliance Department had a person assigned to work with the Social Media team on this very issue. They would take any list of fraudulent and inappropriate accounts and report them to the social networks themselves to confiscate them or have them shut down.

Figure 3: Removing Unauthorised Accounts

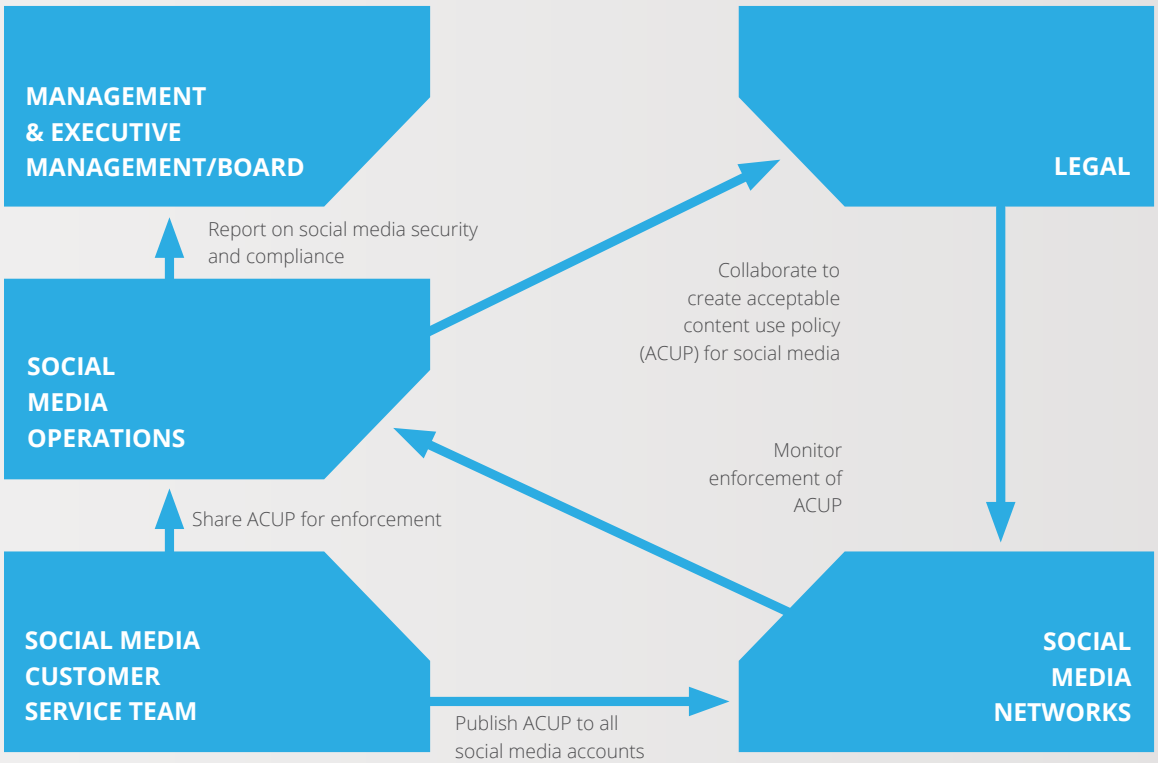


## Case Two: Handling "bad content" moderation

Our bank is a highly visible entity that has garnered a significant amount of social engagement and interaction. As engagement on our Facebook page increased, we recognised the need to remove and hide certain comments on the page to protect commenters when, for example, they inappropriately posted personally identifiable information, account details, and other confidential data to our wall. We also had to remove things like social spam, offensive content, and audience-on-audience abuse or exploitation. It is important to note that these actions were not about removing negativity toward the bank, but about protecting the audience and fostering a positive social community.

First, my Social Media team—in conjunction with the Social Customer Service team—worked with Legal to create a content use policy to publish on our accounts as a link (see Figure 4). After publishing our policy, the Social Customer Service team was responsible for enforcing the policy across our accounts, while our Social Operations team kept reports on bad content moderation activity and published that metric in broader social media reports for our executive stakeholders.

Figure 4: Effective Content Moderation



# Next Steps

The only guarantee is this new age is that every company is at risk. It may be today or it may be next year, but it is more likely than not that a social media risk will manifest itself. To mitigate and minimise the potential impact to your company, you need to act today by doing the following:

## Step 1: Define a governance structure.

Any successful social media risk management and mitigation effort needs a foundation. That foundation is a governance structure. The governance structure is often determined by the head of social media, leading a working group made up of representatives from Marketing Management, IT, Social Media Marketing, Legal and Audit, and Human Resources. The governance architecture, at a minimum, needs to explain who is responsible for what, but should also address items like the scope of your social media efforts, branding guidelines, approval processes, continuity planning, and training and education.

## Step 2: Put a social media policy in place.

A social media policy (or set of policies) that provides guidance for employees and protects the company and customers from risk should come right after governance. This may take the form of a single policy, a set of policies, or even a set of guidelines. The purpose of these policies should be to provide a set of guardrails for all employees, those specifically engaged in social media on behalf of the brand, and managers across the organisation. For a social media policy or set of guidelines to be both useful and usable, the policy should:

1. Be clear in its purpose;
2. Be in sync with the company culture;
3. Explain how the correct use of social media is beneficial to the company;
4. Be written in plain language and not legalese;
5. Have the input and buy-in from all departments; and
6. Be as short and to the point as possible.

## Step 3: Select technologies that will support your organisation.

Once companies have a foundational governance structure in place, then IT departments and social media technology groups can put into place the appropriate tools to manage and mitigate risk. These tools should give the company centralised visibility of all social media accounts and allow administrators to provision limited access permissions for employees, contractors, and agencies. Technologies must also provide governance over which types of content and data are published, ensure compliance with internal policies and external regulations, and protect company accounts and platforms from being hacked.

## Step 4: Test your organisation.

After governance, policies, and technologies are in place, companies need to test and retest to make sure that all the moving parts remain in sync. A “provide and pray” approach to risk management technology is bound to fall short. Organisations must support their employees with ongoing training and up-to-date best practices to ensure that tools are serving business goals. Companies should also test their ability to respond to different scenarios by running a series of simulations based upon known risks. These might range from a situation arising from a mis-sent Tweet, such as a personal statement on a company channel, to a scenario involving an irate customer who takes to social media to voice their issue, to a crisis simulation of a social media-based reputation attack by an NGO, like efforts by Greenpeace against Nestle and British Petroleum.

**About Hootsuite Enterprise**

Hootsuite Enterprise is a social relationship platform for businesses and organisations to collaboratively execute campaigns across social networks such as Twitter, Facebook, LinkedIn, and Google+ Pages from one secure, web-based dashboard. Advanced functionality includes tools for audience engagement, team collaboration, account security, and comprehensive analytics for end-to-end measurement and reporting. To learn more, visit: enterprise.Hootsuite.com.

**About Nexgate**

Nexgate provides cloud-based brand protection and compliance for enterprise social media accounts. Its patent-pending technology seamlessly integrates with leading social media platforms and applications to find and audit brand affiliated accounts, control connected appliances, detect and remediate compliance risks, archive communications, and detect fraud and account hacking.

Nexgate is based in San Francisco, California, and is used by some of the world's largest financial services, pharmaceutical, Internet security, manufacturing, media, and retail organisations to discover, audit, and protect their social infrastructure.

# About Hootsuite Enterprise

Partner with Hootsuite to accelerate your social transformation


Hootsuite Enterprise empowers organisations to execute business strategies for the social media era. As the world's most widely used social relationship platform, Hootsuite Enterprise enables global businesses to scale social media activities across multiple teams, departments, and business units. Our versatile platform supports a thriving ecosystem of technology integrations, allowing businesses to extend social media into existing systems and programs.

We help organisations create deeper relationships with customers and draw meaningful insights from social media data. Innovating since day one, we continue to help businesses pioneer the social media landscape and accelerate their success through education and professional services.

Request a custom demo today by visiting enterprise.hootsuite.com

## Trusted by 744 of the Fortune 1000

WWF · Virgin · Sony Music · Jetstar · City of Melbourne · Seagate · Eurostar · Allianz · Nintendo · Cover-More Travel Insurance · Victorinox · Mashable

Hootsuite™