accenture

Strategy | Consulting | Digital | Technology | Operations

A Comprehensive Approach to Managing Social Media Risk and Compliance

High performance. Delivered.


INTELLECTUAL PROPERTY LOSS
PRIVACY VIOLATION

FOREWORD

Steve Culp
Senior Managing Director
Accenture Finance & Risk Services

SOCIAL MEDIA HAS GROWN IN POPULARITY AND IMPORTANCE FASTER THAN MOST COMPANIES' RISK MANAGEMENT CAPABILITIES CAN CURRENTLY HANDLE.

In one year alone—from 2012 to 2013—the number of social network users around the world rose from 1.47 billion to 1.73 billion (about 25 percent of the world's population), an 18 percent increase. By 2017, the global social network audience is expected to total 2.55 billion.[1] More than 72 percent of all internet users regularly access social networking sites.[2] And, in the UK and US alone, people spend respectively 13 and 16 minutes every hour using social media.[2]

Perhaps more important is take-up of social media by businesses around the world. Among Fortune 500 firms, 77 percent now have active Twitter® accounts, 70 percent have Facebook® pages and 69 percent have YouTube™ accounts.[3]

At issue here is the fact that traditional risk management policies and procedures were not designed for, quite literally, minute-by-minute monitoring of social media chatter to identify brand, strategy, compliance, legal and market risks.

Those risks are considerable. Financial institutions have had to shut down social media forums due to unanticipated negative feedback; the stock markets have been buffeted by fraudulent social network postings; businesses have had to change or rescind strategies in response to the force of social media; other businesses have suffered brand damage due to the power of social media to send negative impressions almost instantly around the world.

This Accenture paper, "A Comprehensive Approach to Managing Social Media Risk and Compliance," acknowledges the power and importance of social media to businesses in every industry. At the same time, it helps identify and explore many of the potential negative consequences posed by social media in terms of brand, strategy, regulatory, legal and market risks. More important, it outlines a holistic approach to identifying, assessing and managing those risks.

Our focus is on distinctive responses—policies, procedures, technologies and competencies—across traditional risk management categories of governance, processes and information technology.

Especially important is the human dimension—creating a risk culture that is attuned to both the significant benefits and the distinctive risks of social media, and putting in place the compliance and performance management capabilities that can lead to changed behaviors in social media usage.

We augment these discussions of methods and best practices with practical advice from risk professionals. These are especially interesting inputs to the discussion because they tap into very timely concerns—such as the global head of privacy and information management for a major US bank discussing how recent regulatory changes require his bank to track social media complaints, even if they have not been officially lodged. As he says, that demand is "taking the industry by storm."

Another of our interviewees notes, however, that it's important for financial services institutions and all businesses to "be bold." Build a social media presence and "create some cool things." In fact, an effective social media risk management capability can bring bold ideas to life and make a difference in the business outcomes your company delivers.

INTRODUCTION: THE BENEFITS AND RISKS OF SOCIAL MEDIA

DID YOU HEAR THE STORY ABOUT THE HACKER WHO FRAUDULENTLY USED THE ASSOCIATED PRESS'S TWITTER® ACCOUNT TO POST NEWS OF AN ALLEGED BOMBING AT THE WHITE HOUSE, CAUSING THE STOCK MARKET TO DROP ABOUT 150 POINTS IN JUST MINUTES?

Or the "pump and dump" stories about people using social media to post fake news about a company's performance, then profiting from the bump in stock price? Or the stories of criminals who have used personal information posted by people on their social media pages to glean answers to security questions and thereby gain access to their bank accounts?[4]

You have probably heard these stories and many others like them. They are evidence of the fact that, however many benefits social media platforms provide for companies in terms of communications, publicity, increased consumer engagement and more, social media also carries with it many risks.

SHORTFALLS IN MANAGING SOCIAL MEDIA RISK

Are companies taking these risks seriously and handling them methodically? The data strongly implies that they are at times overconfident and inadequately prepared. According to a recent survey that looked at corporate social media risks and rewards, almost three out of four executives surveyed (71 percent) said that their company is concerned about these risks but "believe the risks can be mitigated or avoided." Another 13 percent indicated they felt their company does not currently believe it has any appreciable risks.[5]

Of equal concern to this kind of misplaced overconfidence was the fact that 59 percent of respondents reported that they had no social media risk assessment plan in place, and only 36 percent reported offering social media training.[5] What could explain this apparent complacency?

One issue is that a great deal of press coverage is focused on the brand or reputational risk aspects of social media use. But reputational risk is only one among many types of social media risks, and in some cases can hide or obscure other types of risks under a single label of brand value and reputation.

It stands to reason that if companies do not have a broad enough understanding of social media risks, they are likely not to have in place a broad enough approach to managing social media risks.

A COMPREHENSIVE AND PROACTIVE RESPONSE

This paper presents a comprehensive approach to managing these social media risks more effectively. The approach involves structures and actions across several major streams of work, including governance, processes and information systems—supported by leadership, culture, compliance and performance management activities that strengthen the human dimension of risk management, which can often be the weakest link.

Although the paper focuses primarily on the financial services industry, the insights and prescriptions are applicable to most other industries. We have augmented and supported the analyses and recommendations in the paper with insights from several banking executives in areas such as information security, social media and privacy who are working to manage risk effectively while expanding their institution's social media presence. Interviews with these executives were conducted exclusively for this report.

Social media is in many respects an unstoppable cultural force, in spite of some organizations' attempts to block or curtail its use. Because social media is this kind of force—ubiquitous and powerful—it is better to manage it effectively than try to stand in its way.


REGULATORY
RISK
LEGAL
RISK

PART 1: THE RISE AND THE RISKS OF SOCIAL MEDIA

THE NUMBER OF COMPANIES, AND THE NUMBER OF COMPANY EMPLOYEES USING SOCIAL MEDIA APPLICATIONS IS GROWING AT A RAPID PACE.

According to one report,[1] the number of social network users around the world rose from 1.47 billion in 2012 to 1.73 billion in 2013 (about 25 percent of the population), an 18 percent increase. By 2017, the global social network audience is expected to total 2.55 billion. (See sidebar, "Social media in context.")

Among corporations, establishing a social media presence is now more than accepted—it's expected. Among Fortune 500 firms, 77 percent have active Twitter® accounts, 70 percent have Facebook® pages and 69 percent have YouTube™ accounts. About one-third (34 percent) maintain active blogs.[3] Over 90 percent of US companies use social media for recruiting.[7] In the financial services industry, other ways in which social media has value include:

- Branding
- Marketing/advertising
- Corporate communications
- Servicing
- Grievances resolution

A significant sticking point when it comes to properly leveraging social media is dealing with the many risks to which companies are exposed. According to the 2014 RiskTech100 report,[8] published by Accenture and Chartis, reputational and brand risk is the one most often discussed, and certainly it is a serious one. Negative exposure on social media sites, or inappropriate or unauthorized action in the company's name, can result in lost trust and lost revenues.

But underlying these reputational risks lie several other types of serious risk:

- Strategic risk
- Business risk
- Regulatory risk
- Legal risk
- Market risk

If not effectively mitigated, these risks can lead to serious negative consequences including fraud, intellectual property loss, financial loss, privacy violations and failure to comply with laws and regulations. (For more, see sidebar, "Sources and types of social media risks.")

As an example, consider the mix of business, regulatory and legal risks in the following: According to the global head of privacy and information management for a major US bank interviewed for this paper, "The biggest risk for me is our employees disclosing information about our clients on social media. This risk is especially prevalent given the growing presence of Millennials in the workplace, because they are accustomed to sharing personal information and many of their current activities over social media. At times there is over-disclosure of their personal life moments, which can bleed over into their professional life moments, and we need those to be confidential."

Complicating companies' plans to mitigate these risks are several marketplace, technology and organizational factors. For example, the number of social media platforms is growing constantly, which means companies are, as the saying goes, trying to change the tires on a moving vehicle. The complex media environment makes it difficult to integrate with a company's operating model, which means an organization is often reduced to simply reacting to events after they've happened, instead of taking proactive steps.

Finally, social media risks are difficult to quantify. Most corporate initiatives are not approved without a strong business case, but beyond pointing to well-known examples of companies that have suffered losses because of social media, comprehensive cost/benefit analyses are still in their early stages—meaning that many risks still go uncontrolled.

In fact, a standalone business case for managing social media risk is rarely necessary, assuming that companies already have created a business case for expanding their social media operations. Typically the risk assessment that comes with this case involves looking at potential negative outcomes, assessing the damage they could do and then assigning a probability to those scenarios. What is the cost of those risks compared to the costs of not being in the social media game at all?

SOCIAL MEDIA IN CONTEXT

In the words of a senior executive of social media for a major international bank, "One risk is actually not being open enough to social media, actually knowing its role in business and culture. I still hear stories of executives in the industry not taking social media that seriously—that it's just a 'nice to have.' But there is great power in it. This can be negative, given the speed with which issues spread on social media. But it can also be extremely positive. It can foster better relationships or create additional touch points in the digital marketing space."

At the same time, this executive notes that social media "must be understood to be equally important as other channels: radio interviews, TV broadcasts, newspaper and magazine articles, web articles and so on."

Customer and client demographics are among the factors playing a role in the extent to which banks enter the social media arena and at what pace. The Chief Information Security Officer (CISO) for a US regional bank notes, "Social media is a channel, but because of the demographics of our business, at this time it is as important—no more and no less—as, say the branch channel, the call center or online banking. The story here is the demographics of our customer base which tends to be a bit older. For other banks targeting younger and affluent communities, social media is more often prioritized higher than the other traditional banking channels."

For whatever reason and whatever the pace at which a financial institution embraces social media, the channel's many risks must be identified, monitored and managed. To be prevented is a situation in which banks extend their social media exposure before recognizing and anticipating the threats.

SOURCES AND TYPES OF SOCIAL MEDIA RISKS

WHILE OFFERING A HOST OF POTENTIAL BUSINESS BENEFITS, THE USE OF SOCIAL MEDIA CAN EXPOSE COMPANIES TO NUMEROUS BUSINESS RISKS. MOST OF THESE RISKS RESULT FROM A COMBINATION OF ORGANIZATIONAL WEAKNESSES AND VULNERABILITIES EXPOSED THROUGH DATA MISUSE AND DATA SHARING.

FRAUD

Several high-profile cases of hackers representing themselves as organizations or companies have highlighted the potential of social media to perpetrate fraud that is harder to deal with because information goes "viral" so quickly in an online and wireless world. These cases have had serious consequences. Hackers representing themselves on Twitter® as the Associated Press posted a false story about a bombing at the White House which caused the Dow Jones Industrial Average to fall about 150 points in a matter of minutes, representing approximately $150 billion in market value.[9] Several other news organizations have had their online presence compromised through similar kinds of activities.

In other cases a hacker misrepresenting a company has posted fake announcements with exceptional financial news, causing and then profiting from a rise in the company's stock price. These actual cases and their importance have not been helped by a new trend used by several companies which involves "fraudulent fraud"—that is, staging a fake hack as part of a promotional program.[10]

Fraud risks from social media are likely to increase dramatically because of the Security and Exchange Commission's decision in early 2013 to let businesses conduct financial disclosures and release material information over social media platforms such as Twitter® and Facebook®.[11] The stakes are getting higher. Although no penalties are yet in place if a company has vulnerabilities that allow it to be hacked in a way that manipulates a market, this could change. One of the commissioners with the US Commodity Futures Trading Commission has called for fines to be imposed on companies when such things happen.[11] (For more on regulatory compliance and controls, see the sidebar, "A Summary of Social Media Regulations in the US and UK for Financial Services Companies," page 19.)

LOSS OF INTELLECTUAL PROPERTY

Corporate espionage is a thriving business: One estimate is that among the world's 1,000 largest companies, espionage results in $45 billion in losses every year.[12] It's an activity that has been made easier in many ways by the growth of social media.

Source: Accenture, August 2014

To understand why, consider the different ways that data and information can be misused by people. First, it can be misused by people both inside a company and external to it; second, it can be misused or shared accidentally or maliciously.

So the salesperson who establishes LinkedIn® relationships with customers doesn't intend to disclose a confidential and highly valuable customer list, but in effect is doing so. Employees who make a Facebook® posting or tweet about interesting work they are doing may mean no harm; but a good corporate spy might be able to put several such pieces of information together to develop advance information about a company's product that's still at the R&D stage. In one case, spies working for a security consultancy were able to predict that a company would file for bankruptcy based on employee tweets about budget cuts and the fact that the vice president of operations was looking for a job on LinkedIn®.[13] (The irony here is that in some cases LinkedIn® is the only social media site that banks do not block for their employees because they believe it is a "professional networking" site.)

In another case, a spy assumed a different identity and sent a Facebook® friend request to a corporate executive. As the days went by, he dropped his guard and eventually shared non-public information about his company's revenues.[13]

FINANCIAL LOSS DUE TO MALWARE

Because users of social media platforms such as Facebook® so often send links to each other—links to videos, music and so forth—it has become distressingly easy for hackers and spies to install rogue software on computers when people inadvertently click a bad link—including, in some cases, what looks like a legitimate advertisement. Such malware can cause a variety of mischief, including luring people into fraudulent transactions or using hidden software to steal data and personal information, as well as corporate information that might be on the computer.

In another recent trend, hackers are establishing second Facebook® pages for people and companies, thus establishing relationships in which someone might divulge important information. Some other scams have used messaging capabilities within social media platforms to conduct computer attacks.[14]

In other cases, phishing schemes that look like legitimate messages from a social media company result in users revealing their password. Many people use the same password for multiple accounts, which could mean someone now has a password to the person's corporate network.[14]

PRIVACY VIOLATIONS

In some highly publicized cases, social media sites have experienced security breaches in which confidential user information was shared publicly. This happened to Facebook® in early 2013, when a software bug enabled a program to inadvertently share six million users' information such as email addresses and phone numbers. The breach meant that any company that was using Facebook® to promote its business might have had its customers' information shared publicly.[15]

Another way that customer privacy can be violated is through a technique called "data scraping." This is a method of tracking people's activities online and gathering personal data from their use of social media sites as well as online sites. In some cases, this is done by research companies who then sell the data to other companies.

And then there might always be some previously undiscovered back door into a social media application. This happened in 2010 to Foursquare®, the site where users check in to let friends know where they are and what they're doing. A programmer discovered he could write a program mining the photos of users to know where they were almost any hour of the day. Foursquare® fixed the bug, but the sense that social media users are laying down a constant track of information has to give people and corporations pause.[16]


SYSTEMS
PROCESSES
GOVERNANCE

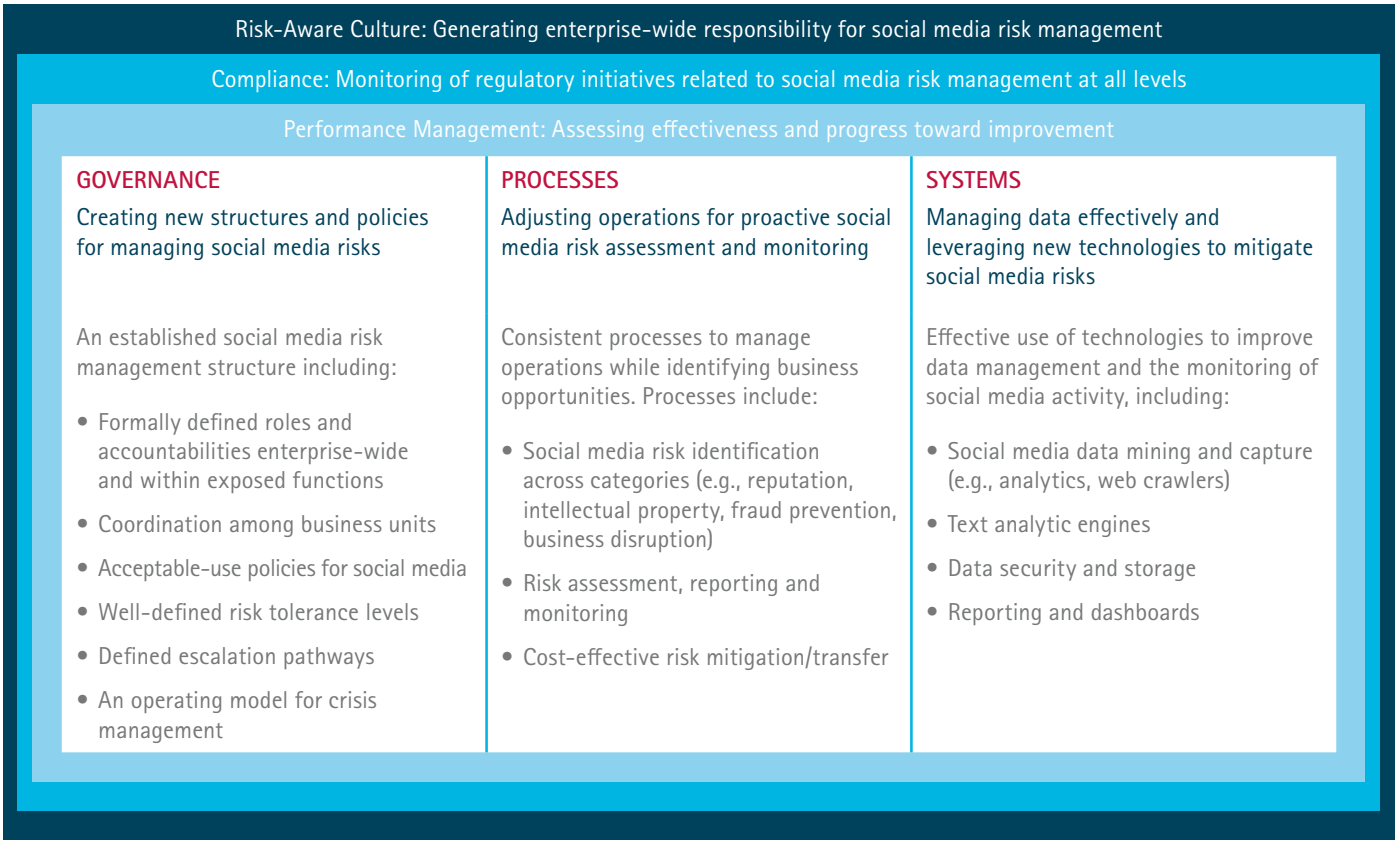
PART 2: THE ESSENTIAL COMPONENTS OF EFFECTIVE SOCIAL MEDIA RISK MANAGEMENT

COMPANIES TYPICALLY ENCOUNTER A NUMBER OF ORGANIZATIONAL WEAKNESSES AS THEY BEGIN TO ANALYZE THEIR VULNERABILITIES TO SOCIAL MEDIA RISKS.

For example, policies governing the use of and access to data may be outdated or weak. Roles and responsibilities for oversight of the various risk dimensions could be unclear. Processes for managing risk are often inconsistent from business unit to business unit or from location to location.

In the face of social media risks and these organizational vulnerabilities, Accenture recommends a social media risk management approach with distinctive activities across governance, processes and systems. (See Figure 1.) These become the value catalysts for realizing the full potential of a social media strategy. The three main components are augmented and supported by other activities having to do with compliance, culture and leadership, and performance management.

FIGURE 1: ACCENTURE'S COMPREHENSIVE FRAMEWORK FOR EFFECTIVELY MANAGING SOCIAL MEDIA RISK



Source: Accenture, August 2014

I. GOVERNANCE

Governance is focused on creating new structures, policies and accountabilities for managing social media risk, as well as the awareness of how the organization is using social media strategically and operationally. Although general governance principles apply in the realm of social media as with other corporate strategies, some specific differences and permutations need to be noted in several areas, including the need to coordinate effectively across functions and the need to have well-defined crisis management procedures that can be instituted at a moment's notice.

DEFINED ROLES AND ACCOUNTABILITIES FOR SPECIFIC TYPES OF SOCIAL MEDIA RISKS

As noted earlier, the risks arising from the use of social media in a corporate environment expose many different functions and groups to risks—from compliance to corporate affairs to IT to marketing. These groups need to cooperate to combat their mutual vulnerabilities, which means sharing information and operating according to consistent policies and understandings.

Part of this shared understanding involves clearly defined roles and accountabilities. In Figure 2, we show a sample or illustrative governance structure which provides an idea not just of the lines of reporting, but also what role each function can play in identifying, assessing and managing particular kinds of risks. The marketing organization, for example, might be primarily focused on brand or reputational risk, while the legal and audit departments would be accountable for privacy issues and fraud, respectively.

As noted by the social media executive for an international bank, it is important to structure the organization and the assignment of responsibilities such that the risk function is always participating in strategic discussions. "We have an extensive risk management network. Each part of the business has its own team, so there needs to be coordination. From a risk perspective, having a central steering group may not always be the most effective way to get things done quickly. However, it is always important to have a representative from risk sitting at the table—someone from compliance, someone from legal, and so forth, to provide guidance to the business and make sure what the company is doing is sound."

COORDINATION WITH OTHER BUSINESS UNITS

Although the banking social media executive had some caveats about the limitations of a central risk group, he went on to speak of the importance of coordinating the social media strategy itself as a means of mitigating reputational and business risks. "We occupy a very large piece of real estate in the social media sphere, covering all our business units. So from that perspective, it is important to have a central group—in our case, the marketing and branding division—that oversees the social media strategy." Larger organizations need to make sure that different units do not post conflicting statements. "It's very important to make sure everyone knows what each other is doing," he concluded.

ACCEPTABLE-USE POLICIES FOR SOCIAL MEDIA

Creating an acceptable-use policy for employees (as well as, potentially, contractors and vendors) when it comes to social media does not involve starting with a blank page, but rather building on existing policies covering media interaction, public communications, the handling of

FIGURE 2: AN ILLUSTRATIVE EXAMPLE OF A SOCIAL MEDIA RISK MANAGEMENT GOVERNANCE AND ACCOUNTABILITY STRUCTURE

Source: Accenture, August 2014

confidential information and how to protect against the misuse of information. (The Social Media Governance organization maintains a database of sample social media acceptable-use statements from more than 200 organizations at: http://socialmediagovernance.com/policies.php.)

In general, such policy statements should encourage, rather than discourage, social media activity, and help provide strong guidelines and examples of behaviors that are acceptable and not acceptable.

However, among the policies that banks need to be wary of is how to reconcile building relationships over social media with their consequent risks. One policy among some banks, as noted by the CISO of a US regional financial institution, is that the bank does not interact with customers (yet) over social media but only through branch, phone or banking channels. Said this executive, "It's vitally important for banks to consider the many risks—including reputation and compliance—that come with customer interaction over social media."

According to the head of privacy and information management for a major US bank, sometimes the goals of the marketing organization and the risk organization may come into conflict. Said this executive, "The bank has been increasing our social media presence for our client-facing staff. Given that emphasis, salespeople might want to establish a LinkedIn® or Facebook® relationship with a client. Although not yet an official policy, we strongly discourage this because of the heightened risk it brings of disclosing private information about clients on a public social media site."

In other cases, social media sites are blocked from a bank's corporate workstations. Although such a policy might be viewed as untrusting or overbearing, the banking social media executive we spoke with offered a different perspective. "When I first joined the bank," he said, "I thought that blocking social media access was a backward step; my attitude was, 'It's a new age, get with the program.'" Earlier in his career, this executive had worked in an industry more reliant on social media. "In a banking environment, however, the risk of personal data getting out is so much greater. So, being blocked from social media by default is not about being Big Brother. After all, an employee can still use a smartphone to access social media. From a policy perspective, this is part of doing everything we can to protect everyone—clients, employees and our stakeholders."

WELL-DEFINED SOCIAL MEDIA RISK TOLERANCE LEVELS

Companies with a mature enterprise risk management function are accustomed to speaking about risk tolerance levels. For example, they set trading limits or, if they are operating in a country where unrest is present, will set a tolerance level about employee safety and when they need to pull employees out.

Similarly, companies need to define what their risk tolerances are for social media. For example, if a company wants to encourage more open engagement with the public at large and get many people talking about their brand, that is an opportunity that carries with it a higher degree of risk; people who do not know the company very well will be making posts visible to thousands of people.

Another consideration is about what kind of information the company is comfortable sharing over social media sites. Does it want to share financial information that increases transparency—something welcomed by suppliers and contractors but which could also expose information to competitors? In general, it is important for companies to run scenarios with outcomes of increasing levels of impact to determine where they want to set limits.

DEFINED ESCALATION PATHWAYS AND REPORTING LINES

It is important to appoint, for each key category risk, an individual who is responsible for making ultimate decisions about social media risks, managing risks and handling any crises that may arise. From the risk owner downward in the organizational structure there should be a clear reporting line—an escalation pathway such that if an indicator of risk appears everyone knows exactly how the issue is to be escalated.

AN OPERATING MODEL FOR CRISIS MANAGEMENT

In a certain percentage of cases, almost inevitably, "risks" become real issues that need to be dealt with. To plan for such an occurrence, companies need what the banking social media executive terms, "an operating model for crisis management." In today's environment, when a customer is dissatisfied, they are now empowered to complain instantly to a large number of people through social media; if a large number of people retweet or repost this information, the bad impression can go viral very quickly.

Two things are especially important in these instances, notes this executive. First, for some types of issues, some messaging and responses need to be pre-written and pre-approved by public relations and the legal department, "so responses can be made very quickly by approved people who are notified of an incident."

Second, for instances when pre-approved responses are not enough, "it is vital to ensure that you're able to get key decision-makers together very quickly and agree on some joint messaging. It's also very important that every stakeholder in social media within a large organization buys into that as well, because if they don't think it has anything to do with them the entire organization could be at risk."

In some cases, continues the executive, "the correct rapid response is a high-level acknowledgment of an issue, with the clear message that you are looking into it and will provide an update as soon as possible. Such an answer can go a long way toward placating dissatisfied people. It's even better if you can give them an estimate as to when you'll get back to them. So managing expectations is very important." In some cases, companies have stumbled in the social area "because they either just went silent or, equally bad, simply pushed out responses without establishing a two-way conversation."

FROM GOVERNANCE TO PROCESSES

Together, these capabilities and structures define an effective governance structure. However, policies and structures only come alive as they become actions. For that, we turn to the second component, processes.

II. PROCESSES

Effective social media risk management processes protect operations and the brand in a cost-effective way—adjusting operations for proactive social media risk assessment and monitoring. Companies are already aware of the importance of having consistent processes in place to handle identifying, measuring, managing and reporting on risks. However, such processes will often look somewhat different in the social media world, in part because of the always-on nature of social networking platforms.

IDENTIFYING THE RISKS OF SOCIAL MEDIA AS WELL AS THE OPPORTUNITIES

Social media risks need to be accurately identified across categories—for example, reputation, intellectual property, fraud prevention and business disruption.

Risk identification builds upon the guidance set forth in this paper's discussion of governance. That is, to identify risks properly requires knowing what the company's risk tolerance levels are for different activities. It means being familiar with policies to understand broadly what the company's attitudes are. And it means understanding roles and accountabilities to bring the right people together to properly and accurately define risks.

Part of risk identification is actually identifying business opportunities. For example, given your institution's known social media risk strengths and weaknesses, what could be done in the way of new products, services, product development partnerships and so forth? What are the opportunities to cut costs or reach customers in new ways? Risk management, after all, is not about suppressing profit-generating activities but rather about properly directing those activities.

ASSESSING AND REPORTING ON RISK FROM DIFFERENT FUNCTIONAL PERSPECTIVES

If we refer back to Figure 2, the illustrative governance structure, another way to understand the responsibilities of the individual functions is to say that they are charged with collecting information, monitoring the risk environment and paying attention to the early warning signals that indicate something could go wrong. The methodology used may differ by function because they are dealing with different channels and platforms. An HR director might be paying attention to sites such as LinkedIn®, while legal might be monitoring email traffic to see if any issues of liability are arising. Marketing would be monitoring various platforms to understand how the brand is being used or discussed by customers.

In each case, however, what is consistent is that companies are identifying, assessing and managing risk and then reporting this up to a social media risk manager who consolidates the information, escalates any issues and effectively audits the process being used by the various functions. The risk manager works to ensure that the groups are monitoring activities with the right frequency and that the data and reports they are providing are of high quality.

MONITORING RISKS CONTINUOUSLY

Senior management needs to be provided with the appropriate information with the right amount of frequency to manage social media risks appropriately. However, risk monitoring is a more complicated process in the social media world than it is with more traditional transactions and communications. Social media is always on, especially for a global business, so monitoring in effect needs to be continuous.

One of the benefits of social media monitoring is early identification of problems that can lead to increased business risk. According to the banking social media executive, "Input from social media can help companies take rapid steps to fix a problem. If you get 500 tweets on a particular issue, those people cannot possibly all know each other, so it's an indication of a real problem that you can then quickly address. With tweets, you can also identify a general geographic area, which also really helps to identify where the issue is occurring."

Some companies are taking advantage of technologies to augment actual human monitoring. Web crawlers can be deployed that use sentiment analysis technology to find references to a company, infer whether the reference is positive or negative and in what context (e.g., customer care, product quality) and report back. In this way, reputational risks can be identified faster and counter-actions put in place quickly.

Other technologies are now helping companies monitor employee activity on social media to assess business risks. For example, many financial institutions are looking into more compliance-related tools that prevent an employee from saying anything on social media that violates a particular regulation. In the UK, Hearsay Social, Inc. offers financial services institutions a platform, integrated with existing systems, to roll out and manage social programs while meeting compliance requirements. In the US, Actiance Inc. provides a platform that helps firms manage social media channels by:[17]

- Controlling access to applications, including authorizations.
- Monitoring social media content to protect brand value and ensure data security.
- Capturing social media conversations in context to provide more robust information.
- Searching all captured content quickly, supporting legal and discovery inquiries.
- Archiving all social media activity captured to support compliance with regulations.

The ability to halt risky social media activity before it becomes a problem is an important feature, notes the banking social media executive. "For example, say a customer tweets you with an issue with their business credit card, and you respond and say if you're having trouble with your credit card, call this number, that tweet will get blocked and rerouted to monitoring. This way a bank knows if the tweet was a promotion or whether it indicated an issue with service."

In some cases, companies have established a social media center of excellence to gather better insights on their customers' needs, understand the perceptions held of their brands and help better engage with customers on social media going forward. For example, a US-based global pharmaceutical company asked Accenture to help set up a regional Social Media Centre of Excellence (CoE) for Europe, Australia and Canada. The center will provide brand, corporate communications and medical teams in the region with strong social media monitoring and engagement support.

Accenture leveraged best-of-breed social media management solutions and its proprietary Social CRM Integration solution to provide a 360-degree social view of the customer, personalized customer support and peer support to drive superior customer satisfaction and reduce operational costs.

MITIGATING AND/OR TRANSFERRING RISKS COST-EFFECTIVELY

A key goal of effective risk management is to decrease the likelihood that risks will occur, as well as improve the capabilities and capacities of the organization—people, processes, technologies and structures. However, it can also mean transferring some or all of the risk elsewhere. This could mean insuring against it—providing some compensation in case of brand damage or protection against directors' liability.

On the other hand, companies may decide that an entire process is too risky for them and that their internal skills are not up to the challenge, which could lead to a decision to outsource the performance of a particular function. (See "Social media monitoring services for a global bank.")

If companies have done their analyses properly of where the risks are, what the indicators are and what the risk tolerance level is, then that should provide them with strong guidance as to whether to mitigate the risk or transfer it.

III. SYSTEMS

Are you capable of monitoring social media networks in real time to identify what is being said about your company and what issues arise from that chatter from the standpoint of regulatory, business and brand risks? Such monitoring is now largely dependent on advanced technology. Improving the effectiveness of IT systems in the context of social media risk management is primarily about improving the management and analysis of data and using new technologies to monitor social media sites as a means of mitigating risks. Vast amounts of data are now on social media platforms and so companies need and want to manage that data effectively. Several capabilities are important here.

SOCIAL MEDIA DATA MINING AND CAPTURE

A number of tools are now available that enable companies to mine data across social media platforms and look for particular kinds of information. Web crawlers, referred to earlier, can extract user data from social networks. Data mining and analytics can turn the apparent randomness and chaos of millions of posts and tweets into information to guide marketers and business strategists.

Data mining of social media can improve business intelligence to provide better services and develop innovative opportunities. For example, data mining can help identify who the influential people are in the social media world, detect groupings of people, sense user sentiments, protect security and user privacy, and help build trust between companies and customers.[18]

TEXT ANALYTIC ENGINES

While crawlers and other tools gather the information or mine it, text analytic engines find meaningful patterns in the data to deliver insights. These engines can also segment information to support better decision making—decisions based on hard data, especially unstructured or "Big" data.

DATA SECURITY AND STORAGE

Social media regulations and technologies present new challenges for storing data—challenges related to architectures and security. These challenges are complicated by the fact that social media is generally based on third-party cloud applications—meaning that a company cannot itself control the security of those applications.

REPORTING AND DASHBOARDS

When data has been mined, analyzed, organized and stored effectively, this enables companies to do reporting in a more effective and timely manner. More comprehensive reporting can bring together multiple performance dimensions into a dashboard, helping management look across factors and see where vulnerabilities and risks are, then make better decisions.

SOCIAL MEDIA MONITORING SERVICES FOR A GLOBAL BANK

This major financial institution had in place a sophisticated monitoring capability for traditional media such as newspaper coverage. However, it needed the ability to adapt its risk management approach in light of its move into social media.

The bank was challenged by not having sufficient skills in-house to move to social media monitoring as quickly as needed.

Accenture now runs social media monitoring for the bank as a managed service. It is based on a global operating model designed to deliver more than a dozen services in four languages for the company's major markets around the world as well as for various local and corporate business functions.

PART 3: ENABLERS OF EFFECTIVE SOCIAL MEDIA RISK MANAGEMENT

A NUMBER OF CAPABILITIES UNDERPIN THE GOVERNANCE, PROCESSES AND SYSTEMS OF EFFECTIVE SOCIAL MEDIA RISK MANAGEMENT. THESE INCLUDE A FOCUS ON LEADERSHIP AND CULTURE CHANGE; A SOCIAL MEDIA RISK COMPLIANCE PROGRAM; AND PERFORMANCE MANAGEMENT CAPABILITIES TO ASSESS EFFECTIVENESS AND PROGRESS TOWARD IMPROVEMENT.

RISK-AWARE CULTURE

One of the critical points to remember about risk management is that, in spite of the importance of governance, processes and technologies, much of risk management is still dependent on people, and therefore people's behaviors must be managed. In the words of a banking social media executive, "Mitigating social media risks is not all about the technology. You can put in as many firewalls as you like, but people still need to be knowledgeable about risks and understand their role in mitigating them."

Consequently, one of the key factors that distinguishes the best social media risk managers from their peers is their commitment to creating and infusing a risk-aware culture—an awareness of how the company is being exposed to social media risks and what each individual must do to help manage those risks. It is also important to conduct more detailed tacit knowledge and training across the corporate culture.

In every industry, people and skills are critical components in achieving risk mastery. One Chief Risk Officer that Accenture spoke to as part of another research initiative placed the challenge of the people dimension on the same level as increased regulatory risk and the challenge of organizational integration. The company has lost a number of critical risk management personnel, and the executive faces the challenge of replacing the knowledge held by those people. In a market where demand for risk management skills remains high, it is important that companies build these capabilities in a broader population and have up-to-date plans to fill key positions promptly when they are vacated.[19] Alternatively, as discussed earlier, a managed services approach can be a way to obtain leading-edge skills and capabilities over the long term.

Effective managers of social media risks emphasize the importance of making risk management part of everyone's daily responsibilities. In a company with a risk-aware culture, people at all levels instinctively look for risks and their impacts when using social media.

Making this happen requires that employees:

- Know the rules and guidelines;
- Adhere to those rules and guidelines; and
- Be held accountable for their performance.

Driving a more risk-aware culture also requires proper objective setting, clear roles and responsibilities, proper training and communication and, most important, a unified message from top management demonstrating its importance.

More specifically, proper awareness and management of risk exposure comes from a properly integrated operating model that links the legal function (for regulation interpretation and guidance), compliance (for program design and implementation), operational risk (for proper control and governance), business heads (for implementation and accountability), internal/external audit (as a third line of defense and testing), and technology (for automation and preventive controls that reduce human error). Managing all these moving parts effectively does not happen overnight or as a one-time exercise, but rather operates in a cycle of continuous improvement.

Leadership and sponsorship are equally important to creating a culture attuned to social media risks. A story told by one of our interviewees is a reminder that it is important to bear in mind generational differences that will persist—at least for a time—when it comes to social media and leadership. A US bank's head of privacy and information management spoke of the work he did to understand this gap and to bridge it in a way that created change sponsors among the executive team. He says, "We had a long look at social media from a culture perspective. I facilitated a conversation with our senior management group. Interestingly, no one in the room actually had a Facebook® or Twitter® account. When asked their opinion about approving the use of social media, half said yes and half said no. Technology and HR were in the yes column because they used social media to connect with partners and to recruit, respectively. But the others didn't see the need."

The executive then met with the bank's youth affinity group, a team of high-potential younger professionals. Not surprisingly, 100 percent of them had Facebook® and Twitter® accounts, as well as a presence on other social media platforms. So, part of building strong leadership and sponsorship when it comes to social media, concluded the executive, is understanding not only your current customer demographics, but also what those demographics will be in 10 years.

COMPLIANCE

The complex regulatory landscape regarding social media was discussed earlier, and the accompanying table (page 19) summarizes recent regulatory rulings regarding social media in the US and UK. Many companies find it challenging to manage and comply with multiple regulatory agencies, differing interpretations of regulations, and varying degrees of guidance on regulatory compliance.

On the other hand, as one of our executive interviewees noted, another way to look at social media compliance is that it is simply an extension of things banks are already doing. According to this CISO, "We've done a deep dive into the regulatory guidance for social media. The good news is that the implied guidance is: go back to what the bank does normally in handling complaints, suspicious activity and inquiries from customers at large. Make sure that you comply with extant requirements; file regulatory claims and suspicious activity reports; make sure that you get the Consumer Financial Protection Bureau involved; and make sure that your complaint process is well vetted and well thought through."

In other words, an effective social media risk compliance program should not differ significantly from other compliance risk management programs. A compliance risk framework should include:

- Proper governance and oversight
- Policies and procedures
- Risk assessments
- Risk monitoring
- Testing
- Metrics and reporting

The compliance risk framework is designed to serve as a "safety net" to identify and capture emerging risks that could negatively impact a company's financials, reputation and systems.

One thing important to understand is what's different in the social media arena than in other areas of compliance. According to the global head of privacy and information management for a major US bank, in the US a recent change from the Consumer Financial Protection Bureau (CFPB) is that financial institutions are now required to track complaints that occur on social media—even if the complaint has not been lodged officially to the regulator or to the financial institution itself. Web crawler technologies, discussed earlier, can help by looking for key words and phrases for further analysis and reporting, but complaint tracking is a huge task and responsibility that is, in his words, "taking us all by storm."

PERFORMANCE MANAGEMENT AND MEASUREMENT

Integrated risk performance management is essential if leadership at all levels is to have an end-to-end view of social media risks, their impacts, and their ability to be mitigated or controlled.

A framework for effective performance measurement in a social media risk management context includes:

- Identifying risks (emerging/emerged/realized) through data mining, trend analysis, systems and security.
- Reporting on risks (visibility, accountability, awareness).
- Managing risks (policies, procedures, preventive and detective controls, transfer or sharing of risk).
- Measuring performance of risk mitigation (benchmarks, key risk indicators and key performance indicators).
- Identifying opportunities to improve control effectiveness, reduce exposure and automate processes.

Some fear that a performance management and measurement capability could stifle innovation, something critically important to delivering a successful social media strategy; however, in fact, a proper performance management approach framework can actually enable people and the entire organization framework to pursue new approaches with proper protections in place.

With effective measurement and control capabilities, risk management procedures and a risk-aware culture, companies should be positioned to exploit future opportunities to leverage social media as a customer channel.


COMPLIANCE
RISK-AWARE CULTURE
PERFORMANCE MANAGEMENT

PART 4: CONCLUSION

INSTITUTIONS LOOKING TO ADVANCE THEIR SOCIAL MEDIA RISK MANAGEMENT CAPABILITIES RAPIDLY CAN FOCUS ON SEVERAL KEY INFLUENCE POINTS:

1. Assess vulnerabilities arising from social media use beyond just reputational risk. Consider how social media activity can expose the organization in terms of business, regulatory, legal and market risks.

2. Expand existing risk governance structures and activities to include social media activity. Define risk tolerance levels and acceptable-use policies and have in place effective means for issue escalation and crisis management where necessary. A decentralized governance model can lead to inconsistency in how social media policy is interpreted and implemented, so institutions should ensure governance structures cross organizational lines, making every part of the organization aware of what others are doing. Set a single point of accountability in the governance structure that crosses lines of business.

3. Establish advanced social media monitoring tools and technologies. These enable the risk organization to (a) collect data from various social media sources; (b) analyze unstructured data (such as information about customer sentiment) to enhance monitoring; (c) provide insights into the company's overall risk situation; and (d) measure social media risk exposure according to the institution's risk appetite.

4. Enhance existing performance management capabilities to analyze and act on the metrics delivered from monitoring activities. These metrics are defined based on different models that consider, for example, the use of crisis-scenario analysis and/or the decomposition of risk factors that may affect company's overall risk picture. The focus of risk measurement should be on defining how well controls are performing and where control improvement opportunities may exist.

5. Engage in enterprise-wide change management activities to create a more risk-aware culture. In our view, the most important (and most difficult) aspect of social media control centers on cultural awareness and change. Setting proper expectations and engaging in culturally aware implementation can have a great impact on social media risk control. Establish influential leaders in sponsorship positions to drive awareness and acceptance of the organization's overall monitoring of social media use. Conduct training initiatives that use action learning principles, guiding employees at all levels toward behaviors that are more likely to decrease overall risk.

As one of our executive interviewees noted, social media can offer considerable advantages to financial institutions and most other types of companies. As the executive said, "My advice is to be bold." Establish a presence on the most-used social platforms and "think about creating some cool things."

The other advice: learn to listen. "Listening is absolutely critical for any company that wants to take social media seriously—listening to what people say to them and what they say about them. It's very important to have the ability to analyze who is saying what, and then to be able to dig deep into it, establishing trusted relationships and improving the business at the same time."

Yet, inherent in the use of social media are serious risks—reputational, business, strategic, regulatory and more. To mitigate these risks and to get more value from a social media strategy, companies need to institute governance structures, processes and technologies unique to meeting social media challenges.

A SUMMARY OF SOCIAL MEDIA REGULATIONS IN THE US AND UK FOR FINANCIAL SERVICES COMPANIES

Areas (by agency)	Objectives	Impacts
GOVERNANCE		
Federal Financial Institutions Examination Council (FFIEC)	• Policies and guidelines for advertisement content, selection of third parties, staff training and clear preview of roles and responsibilities • Policies and procedures for data monitoring	• Enhanced control and monitoring of third parties • Changes to risk management framework • Enhanced data monitoring capabilities
Financial Industry Regulatory Authority (FINRA)	• Firms must adopt policies to ensure that persons participating in social media sites are appropriately supervised, have the necessary training and background to engage in such activities and do not pose a risk	• Enhanced HR polices for internal staff and training for third-party staff
Securities and Exchange Commission (SEC)	• Restrictions and prohibitions regarding the use of social media sites by investment advisers based on the firm's analysis • Check appropriateness of pre-approval requirements—either after-the-fact review or before publication	• Changes to existing content monitoring and approval process • Changes to sales and marketing guidelines for investment advisers
Financial Conduct Authority (FCA)	• Social media includes any real time financial promotions like interactive dialog or telephone conversation • Social media includes any non-real time financial promotions like email	• Changes to sales and marketing guidelines on usage for social media channels
DISCLOSURE		
Federal Financial Institutions Examination Council (FFIEC)	• Disclosure of privacy policy • Regulations for unsolicited commercial messages (spam) and unsolicited communications by telephone or SMS	• Control in content approval for external communication and external reporting • Changes to sales and marketing channels as well as third-party guidelines for sales
Securities and Exchange Commission (SEC)	• Publish corporate website address and disclosures on external reports • Disclosures on corporate websites identifying the specific social media channels for company usage	• Changes to public relations, corporate communications and external reporting guidelines • Robust approval process of content on social media sites
PRODUCTS		
Federal Financial Institutions Examination Council (FFIEC)	• Requirements to control misleading, inaccurate or misrepresentation of information • Requirements for control of advertisement content	• Enhanced control over approval and publication of sales, advertisement and product content • Changes to document retention policy
SALES, MARKETING AND DISTRIBUTION		
Federal Financial Institutions Examination Council (FFIEC)	• Obligation on operators of commercial websites content and disclosure of personal information collected from children • Collection of medical and loan information	• Process level changes for sales, marketing, underwriting and legal • Control of content approval

Areas (by agency)	Objectives	Impacts
SALES, MARKETING AND DISTRIBUTION		
Financial Industry Regulatory Authority (FINRA)	• Policies and guidelines for advertisement content • Firms should consider prohibiting all interactive electronic communications that recommend a specific investment product and any link to such a recommendation unless a registered principal has previously approved the content	• Robust controls over advertisement content, third-party marketing and sales procedures • Enhanced guidelines for marketing and sales content
Securities and Exchange Commission (SEC)	• Investment advisers, part of a larger financial services or other corporate enterprise may create guidelines designed to prevent the advertising practices of a firm-wide social media site from violations of the Advisers Act	• Robust approval process of content on social media sites • Changes to sales and marketing guidelines
Financial Conduct Authority (FCA)	• When designing websites and other electronic media, firms should be aware of the difficulties while reproducing certain colors and printing certain types of text • A firm should refer to legislation such as the Data Protection Act 1998 and the Computer Misuse Act 1990	• Changes to sales and marketing guidelines on usage for social media channels • Changes to third-party support for marketing content
PAYMENTS		
Federal Financial Institutions Examination Council (FFIEC)	• Bank Secrecy Act/Anti-money laundering (AML) programs to provide controls to ensure financial transaction ongoing compliance • Training requirements from operation staff to board level	• Enhanced AML process • Enhanced monitoring and recording of suspicious transaction and customer activities
INFORMATION MANAGEMENT		
Federal Financial Institutions Examination Council (FFIEC)	• Requirements to monitor and control content on a site owned or administered by a third party • Procedures to address risks from public posting of confidential or sensitive information	• Enhanced control over data and changes to existing system to monitor data
Financial Industry Regulatory Authority (FINRA)	• Requirement for record retention purposes, the content of the communication is determinative and a broker-dealer must retain those electronic communications that relate to its "business as such"	• Changes to current IT systems for recording and retention of social media data • Changes to current information retention guidelines
Securities and Exchange Commission (SEC)	• Retain records of communications • Guidelines to create appropriate firewalls between sensitive customer information, as well as the firm's own proprietary information, and any social media site to the extent that the firm permits access to such sites by its investment adviser representatives (IARs)	• Incorporation of business intelligence concepts in risk management guidelines • Changes to information retention policy and systems for investment advisers

Source: Accenture analysis based upon publicly available information[20]

NOTES

1. "Social Networking Reaches Nearly One in Four Around the World," eMarketer Inc., June 18, 2013. Access at: http://www.emarketer.com/Article/Social-Networking-Reaches-Nearly-One-Four-Around-World/1009976.

2. "The Growth of Social Media in 2014: 40+ Surprising Stats [Infographic]," Socially Stacked, January 23, 2014. Access at: http://www.sociallystacked.com/2014/01/the-growth-of-social-media-in-2014-40-surprising-stats-infographic/#sthash.t4GoW1Bc.KxNuUnDR.dpbs.

3. "Social Media Use Growing Among Fortune 500 List With 77% Tweeting & 70% On Facebook," Amy Gesenhues, Marketing Land, July 23, 2013. Access at: http://marketingland.com/fortune-500-companys-social-media-use-on-the-rise-52726.

4. "A Single Fake AP Tweet Can Apparently Crash the US Stock Market," Brian Merchant, Motherboard, April 23, 2013. Access at: http://motherboard.vice.com/en_ca/blog/a-single-fake-ap-tweet-can-apparently-crash-the-us-stock-market. "Pump-and-Dumps" and Market Manipulations," U.S. Securities and Exchange Commission. Access at: http://www.sec.gov/answers/pumpdump.htm. "What's dangerous about social media?" Halifax bank. Access at: http://www.halifax.co.uk/aboutonline/security/common-threats/social-media.

5. "Survey: 71% of Companies Concerned Over Social Media Risks, But Only 36% Provide Employee Training," Amy Gesenhues, Marketing Land, September 27, 2013. Access at: http://marketingland.com/survey-71-of-companies-concerned-about-social-media-risks-only-36-do-social-media-training-60212.

6. "Global Risk Management Study 2013: Risk Management for an Era of Greater Uncertainty," Accenture, September 2013. Access at: http://www.accenture.com/microsites/risk-management-research/2013/Pages/home.aspx.

7. "92 percent of Companies Use Social Media for Recruiting. Are You? [Infographic]," Jennifer Beese, Sprout Social, October 17, 2013. Access at: http://sproutsocial.com/insights/social-media-recruiting-infographic.

8. "Chartis: RiskTech100 2014" report, published by Accenture and Chartis, May 2014. Access at: http://risktech-forum.com/research/chartis-risktech100-2014.

9. "A Single Fake AP Tweet Can Apparently Crash the US Stock Market," Brian Merchant, Motherboard, April 23, 2013. Access at: http://motherboard.vice.com/en_ca/blog/a-single-fake-ap-tweet-can-apparently-crash-the-us-stock-market.

10. "Chipotle's Twitter 'Hack' Was A Planned Promotion," Matt McGee, Marketing Land, July 24, 2013. Access at: http://marketingland.com/chipotles-twitter-hack-was-a-planned-promotion-53113.

11. "The truth about social media for business: It's a risk," Verne Kopytoff, Fortune, April 29, 2013. Access at: http://tech.fortune.cnn.com/2013/04/29/the-truth-about-social-media-for-business-its-a-risk.

12. "Social Media and Corporate Espionage," David Albrecht, The Summa, October 28, 2011. Access at: http://profalbrecht.wordpress.com/2011/10/28/social-media-and-corporate-espionage.

13. "The Spy Who Liked Me," Kashmir Hill, Forbes, November 2, 2011. Access at: http://www.forbes.com/sites/kashmirhill/2011/11/02/the-spy-who-liked-me/#./?&_suid=139938961002708059584548958092.

14. "The Legal Implications of Social Networking Part Three: Data Security," David Navetta, InfoLawGroup, January 9, 2012. Access at: http://www.infolawgroup.com/2012/01/articles/social-networking/the-legal-implications-of-social-networking-part-three-data-security.

15. "Facebook Data Breach Exposes Information of Six Million Users," iPost.com, June 24, 2013. Access at: http://www.ipost.com/blog/cloud_computing/facebook-data-breach-exposes-information-of-six-million-users.

16. "Top 5 Privacy Violations of 2010," Jeffrey Evans, Huff Post Tech, December 30, 2010. Access at: http://www.huffingtonpost.com/jeffrey-evans/top-5-privacy-violations-_b_802615.html.

17. "Hearsay Social Delivers Technology Innovation and Industry-Leading Methodology Helping Advisors and Wholesalers Grow Business and Relationships on Social Media," Hearsay Social press release, April 10, 2014. Access at: http://hearsaysocial.com/press-release/hearsay-social-delivers-technology-innovation-and-industry-leading-methodology-helping-advisors-and-wholesalers-grow-business-and-relationships-on-social-media. "Financial Services – Compliance and engagement for the world's most regulated businesses," Actiance web site. Access at: http://www.actiance.com/solutions/financial-services.

18. "Mining Social Media: A Brief Introduction," Pritam Gundecha and Huan Liu, Tutorials in Operations Research, INFORMS 2012. Access at: http://www.public.asu.edu/~pgundech/book_chapter/smm.pdf.

19. "The Risk Masters," Steve Culp, Accenture Outlook Journal 2011, No. 3. Access at: http://www.accenture.com/us-en/outlook/Pages/outlook-journal-2011-risk-masters-risk-management.aspx.

20. "Federal Financial Institutions Examination Council, Docket No. FFIEC-2013-0001, Social Media: Consumer Compliance Risk Management Guidance," Federal Financial Institutions Examination Council. Access at: http://www.ffiec.gov/press/Doc/FFIEC%20social%20media%20guidelines%20FR%20Notice.pdf.

"Mortgages and Home Finance: Conduct of Business Sourcebook (MCOB)," Financial Conduct Authority. Access at: http://fshandbook.info/FS/html/FCA/MCOB.

"National Examination Risk Alert, Investment Adviser Use of Social Media," Volume II, Issue 1, January 4, 2012, Office of Compliance Inspections and Examinations. Access at: http://www.sec.gov/about/offices/ocie/riskalert-socialmedia.pdf.

"Social Media Web Sites, Guidance on Blogs and Social Networking Web Sites," Regulatory Notice, 10-06, January 2010, Financial Industry Regulatory Authority. Access at: http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p120779.pdf.

ABOUT THE AUTHORS

Steve Culp is the senior managing director of Accenture Finance & Risk Services. Based in Chicago, he has more than 20 years of global experience working with clients to define strategy and execute change programs across a broad spectrum of risk management and finance disciplines. Steve is responsible for leading the global group across all dimensions, from setting the strategic direction through to the enablement of local teams operating across diverse markets. In addition, he oversees Accenture's efforts on large-scale transformation programs across Finance and Risk for some of our most important financial services clients.

Prior to his current role he was responsible for our Global Risk Management Practice, and prior to that he led Accenture's Finance & Enterprise Performance consulting services for global banking, insurance and capital markets institutions. With his extensive experience in the financial services industries, combined with his knowledge of risk management and the finance function, he guides executives and client teams on the journey to becoming high-performance businesses.

Rafael Gomes is a senior manager, Finance & Risk Services. Based in London, Rafael specializes in regulatory, reputation, and political risk management and compliance. He works with major financial services institutions to develop risk-based strategies, compliance controls and conduct surveillance programs to manage hard-to-quantify risks. His recent focus has included guiding financial institutions on how to assess and mitigate internal and external risks associated with social media and "big data" programs.

Jonathan Narveson is a senior manager, Accenture Finance & Risk Services. Based in Charlotte, North Carolina, he serves as the Operational Risk Management Capability Lead for North America and has a breadth of experience leading programs related to regulatory compliance, compliance risk management, and operational risk. Most recently, Jon has focused on the evolution of risk management operations, centering on key emerging risk topics such as social media risk management, and helping large financial institutions derive value out of regulatory mandates.

ACKNOWLEDGEMENTS

The authors would like to thank Accenture employees Laura Bishop and Sarah Waylett for their contribution to this document.

ABOUT ACCENTURE

Accenture is a global management consulting, technology services and outsourcing company, with more than 323,000 people serving clients in more than 120 countries. Combining unparalleled experience, comprehensive capabilities across all industries and business functions, and extensive research on the world's most successful companies, Accenture collaborates with clients to help them become high-performance businesses and governments. The company generated net revenues of US$30.0 billion for the fiscal year ended Aug. 31, 2014. Its home page is www.accenture.com.

STAY CONNECTED

Join Us

https://www.facebook.com/accenturestrategy

http://www.facebook.com/accenture

Follow Us

http://twitter.com/accenture

Watch Us

www.youtube.com/accenture

Connect With Us

https://www.linkedin.com/groups?gid=3753715

02-9163 / 14-3979