BITS

FINANCIAL SERVICES ROUNDTABLE

SOCIAL MEDIA RISKS AND MITIGATION

June 2011

BITS
A DIVISION OF THE FINANCIAL SERVICES ROUNDTABLE
1001 PENNSYLVANIA AVENUE NW
SUITE 500 SOUTH
WASHINGTON, DC 20004
202-289-4322
WWW.BITS.ORG

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Social media is a term used to define the relatively recent phenomenon of mass personal publishing most often intended for public consumption and typically conducted in an interactive and conversational style. Social media's rapid growth – it is now the most popular online activity – has garnered the attention of the commercial space, including financial institutions hoping to meet their customers' evolving needs and expectations through this medium.

Recognizing the rapid adoption of social media exemplified by now familiar sites Facebook, Twitter, and LinkedIn, BITS has developed this paper to provide financial services companies with insight into the various risks associated with the deployment and use of social media. This paper does not intend to cover every situation an organization might encounter, but instead serves to highlight the issues common to many financial institutions and provide guidance on how these risks might be moderated.

This paper is intended for a general audience, from business practitioners to compliance, risk and legal professionals, primarily from a United States perspective. It provides a synopsis of the major themes an FI should consider when using and deploying social media and is best used as a reference guide, delving into the situation or organizational section that is most appropriate to the reader. To assist readers in identifying which sections are most applicable to their purpose and expertise, a risk matrix is provided in Appendix E.

This paper addresses risks and mitigation methods for financial institutions using social media from three perspectives:

- To communicate with or service customers,
- By employees within a financial institution in personal and professional capacities, and
- By employees or contractors outside the office.

DISCLAIMER: This document was not created to provide legal advice and all information should be used in consultation with an organization's compliance and legal departments.

INTRODUCTION

Definition
For purposes of this paper, the term Social Media shall include any form of online interaction that allows for the highly scalable publication of user-generated content of any kind (test, audio, video, images) that is meant for general public consumption and uses interactive dialogue with others. It is differentiated from traditional online publication in that the communication tends to be more dynamic, personal and interactive.

History
While much has been made of the recent growth of social media, the core capabilities can be traced through a long lineage of electronic communication. The use of electronic media to communicate broadly is not a phenomenon which began with MySpace and Facebook or even predecessors such as Friendster. The establishment of the Arpanet, a precursor to the modern Internet, was in part driven by the need to collaborate among university and government researchers. From the first message sent in 1971, email has been a common form of social media, particularly when the communication goes beyond a one-to-one correspondence. Email as a social media mechanism expanded through the use of list services (listservs) where the senders and/or recipients may not be directly known and may change over time, often without the knowledge or consent of the participants. More recently, the use of blogs, wikis and other online publications parallels the functionality found in contemporary forms of social networks such as Twitter. In fact, Twitter is classified as a derivative of blogging known as "micro-blogging" with user posts limited in length. Therefore the rise of social media should not be considered isolated or unique, but rather an evolution of online communications with special considerations when used in a very broad and public setting. Moreover, the controls requirements may also not be unique, but their application may be challenged given the ways in which these technologies are deployed. For financial institutions what has changed is the breadth of adoption and ongoing usage by both customers and employees.

Social Media and Its Purposes
Social media is often viewed as a personal communication tool. From a personal user perspective, the use of social media as a means to communicate with friends and relatives, either replacing or in addition to existing communication methods such as email, has been monumental. The ease by which social networking sites allow people to keep up with current acquaintances and reconnect with old friends provides some insight into the popularity of this phenomenon.

In addition to purely personal uses, some sites have tapped into users' professional needs and help individuals build and maintain professional networks. Such capabilities have altered the landscape of how people connect with peers or conduct employment-related activities such as looking for a new job or recruiting and hiring people to fill the needs of an organization.

Because of the impressive adoption of social media by the general public, institutions are realizing this medium can provide business benefits. By connecting with existing and future customers where they spend their online time, businesses are simply echoing the golden rule of real estate within the virtual environment – location, location, location. Communicating with and providing services to customers where they are allows for access, timely conversations, and the hope of a better and more relevant customer experience.

SOCIAL MEDIA RISKS, RISK SCENARIOS AND MITIGATION RECOMMENDATIONS

I. COMPLIANCE

A. Foreign and Domestic Privacy Laws

Description
Companies and individuals often have different, if not altogether conflicting, perspectives on the topic of privacy. Companies want to protect their sensitive information, but some believe an employee has no right to privacy on social media sites, as is the case with casual monitoring. Furthermore, the perception and definition of privacy among individuals can be highly subjective. Questions about privacy rights have only intensified with the emergence of rapid communications such as social media.

Regardless of how companies and individuals define or perceive privacy, companies need to understand the privacy and protection laws, including those in countries in which they do business. With the increasing volume and depth of personal information available online come increasing risks to privacy. For financial institutions, particularly those operating multi-nationally, the sheer number of laws and regulations related to privacy pose challenges to the adoption of information-based services including social media. The scope and jurisdiction of such laws can be influenced by, among other factors, the location where such data is stored or processed or by the nationality of the individual.

Globally, governments have attempted to address individuals' privacy concerns in both the public and private sectors:

- The United States has primarily leveraged existing legislation about privacy through the United States Privacy Act of 1974, which remains a reference point for privacy-related legislation. It establishes certain principles about individual rights, such as:
  - an individual's right to access information that is collected about him or her
  - notice of collection of the data
  - restrictions on how the data are shared
  - legal redress to remedy violations of the stated rights.

- The principles of the Privacy Act of 1974 were codified and augmented in *Fair Information Practice Principles* in the United States under the Federal Trade Commission in the mid 1980s by updating the original Privacy Act.

- Privacy further came to the forefront in the Internet age when dissemination and collection of data became common business practice. For financial services companies, privacy hit center stage in the Financial Modernization Act of 1999 (a.k.a. Gramm-Leach-Bliley Act/GLBA), which established privacy protections regarding the sale and sharing of personal information and codified protections against "pretexting" or the practice of obtaining personal information under false pretenses.

- Outside the United States, other governments have adopted aggressive privacy legislation. Notably, the European Union (EU) law 'forbids the casual monitoring of employees without express consent by the employee and respective council.' The EU's Data Privacy Directives describe data privacy as a basic human right as expressed in Article 8 of their Charter of Fundamental Rights. First established in the mid 1990s, the EU Data Privacy Directive is currently under review, which includes a new concept of the "right to be forgotten" or the right to demand deletion of data no longer needed for its original purpose.

- Many other countries and regions have also established privacy frameworks including Canada's Privacy Act and Charter of Rights and Freedoms and the Personal Information Protection and Electronic Documents Act (PIPEDA) (2000), Australia's Privacy Act of 1988, Asia Pacific Economic Corporation (APEC) Privacy Framework (2004) and others.

When using social media to conduct business, financial institutions must weigh regulatory and legal obligations against their wish to serve their customers or meet business goals. This balancing act is particularly challenging given that the primary purpose of social networking is the broad disclosure of information, including individuals' personal information.

Mitigation

Before adopting any kind of social media to communicate with stakeholders, companies must:

- Create social media policies, including those relevant to privacy issues
- Communicate to and train employees on social media policies and the risks related to privacy
- Consider whether a particular platform is appropriate for the nature of the interaction or information being shared.

Social media policies must be created, including those related to privacy issues. Financial institutions should raise privacy awareness as part of the communications strategy in the implementation of such policies. It's incumbent on a company to review its customer verification practices and continually raise employee and customer awareness about the risk of disclosing sensitive information to unauthorized parties.

For all associates, organizations should:

- Raise general awareness of best practices for protecting privacy on social media sites
- Provide guidance on how to find and use privacy controls on popular social media sites (http://www.sophos.com/en-us/security-news-trends/security-hubs/social-networks.aspx)
- Relate how data aggregation across various social media sites may lead to incremental private information disclosures.

For associates who deal directly with customers, organizations should additionally:

- Review customer verification procedures in light of common data shared via social media.

When engaging customers through the use of social media, companies should think through the following:

- What information are customers requesting though social media? Such information passes through systems that may not match the data-protection measures used by financial institutions.
- Be aware of authorities granted to social media sites such as perpetual license to provided information. While your use of collected information may align with your stated privacy practices, the social media provider's use may not.
- Do customers understand when their communications are operating under a social media site's privacy rules and not those of the institution? It's important that a company clearly state the applicable privacy rules on every site where it maintains a presence.
- As social media evolves how will news services or features affect social media privacy practices? For example, the use of mobile or geo-location information may be considered an encroachment on customer's privacy.
- Remain vigilant about changing privacy settings on any given social media site where you maintain a presence to avoid sharing information with an unintended audience.
- As social media providers undergo mergers and acquisitions, there is the additional concern about how customer data will be shared and/or protected under the new entity. The aggregation of data in such cases could lead to further erosion of information privacy for both individuals and organizations.
- What personal information customers disclose in their personal use of social media. While companies use such information to verify customer identity, customers should be cautioned against sharing private data through social media sites.

B. Managing Compliance with Other Company Policies

Description

The current Internet experience, often called Web 2.0, is being defined by high interactivity, mobile access and the ability to meet your customers in channels of their choice. Marketing is being changed through user-generated content, collaboration and peer-production. This is not business as usual for most financial institutions. While most financial institutions already have existing policies that provide guidelines for associate behavior in social settings both online and in the workplace, most institutions are creating separate social media policies to specifically provide governance for associate use in the social media realm. These new social media policies need to mesh with existing corporate policies and ensure consistent guidelines to associates and third parties.

Corporate policies often do not extend to cover employees' personal behavior outside of the office. In this sense, as employees intermingle their personal and professional lives online, companies need to account for the expanding reach prompted by social media use. Moreover, when emerging social media policies reference other existing policies, the distinction of scope should be considered.

Below are examples of areas which should be assessed for social media context:

- Code of Conduct/Ethics Policies

- E-Commerce Policies
- BSA/AML
- Sarbanes-Oxley Policies
- Privacy Notices
- Marketing, Brand, Logo Enforcement Policies
- Trademark and Intellectual Property Policies
- Legal Risk Policies
- Risk Management Policies
- Promotion, Contest and Sweepstakes Policies
- Employment Verification/ Professional Reference Policies
- External Communications Policies
- Information Security Policies
- Securities Law Policies
- Solicitation and Distribution Policies
- Equal Employment Opportunity Contracts

Mitigation

- Social media policies should explicitly state when other internal policies apply when it comes to social media use.
- Social media policies should be clear on the ramifications of policy violation such as disciplinary or other action.
- Monitoring should be considered to detect associate non-compliance with internal policies.
- Associate relations and managers should be engaged when non-compliance is detected.
- A well established and ongoing awareness and training program should accompany any changes to policy, especially in areas as nuanced as social media.

C. Information Retention Management

Description

Financial institutions are subject to a variety of legal and regulatory obligations. Some of these deal with the practice of retaining and disposing of data. Often there are stipulations on what information is required to be saved for archival and recovery purposes and for what minimal duration. The use of social media introduces another vehicle of communications, and hence information, that is subject to such requirements.

Data retention is not a new practice for the financial community. Regulators have long identified the requirement to capture and retain specific forms of communication, such as advertisements, for prescribed periods of time. For example, NASD/FINRA 3110 and associated SEC 17a-4 identify the need to preserve book, accounts, memoranda and correspondence for broker-dealers.

But changes new communications have introduced or at least enhanced lead to questions of practice and applicability. Is using the Facebook "Like" capability on an article on a popular financial news site a retainable form of communication? Could this action be considered an endorsement and subject to particular regulatory oversight and retention requirements?

As social media primarily occurs on public websites, the ability to capture data which may be subject to retention becomes increasingly difficult. Many sites may not provide capabilities for financial firms to collect data for preservation. Additionally, social media is a very loosely defined and rapidly evolving medium which further exacerbates the ability to meet retention obligations and raises many questions. With the ability of posts, tweets and other communications to be quickly deleted and modified, what obligations are expected of firms to capture data in real-time as opposed to regular snapshots? Additionally, social media sites quickly add and remove features, including adding or removing protections for communications. In such an environment when previously private communications are exposed publicly due to a change in policies of a given social media provider, how quickly are firms expected to retain such communications?

Challenges

Financial institutions have had to deal with data retention requirements in the past, but the use of social media presents several challenges. These include but are not limited to:

- Associates might be able to access social media from both within and external to the financial institution. This may preclude the use of traditional data capturing capabilities at "choke-points" within a data network for inspection and retention purposes.
- The volume of data on social media quickly raises resource needs, particularly when dealing with multi-media within social media to include photographs, videos and audio in addition to text-based information.
- The number of social media platforms and sites continues to grow with no standard formats in comparison to traditional electronic communications such as email.
- The tight integration of both personal and professional communications on many social media platforms might raise privacy and over-retention concerns through the inability to distinguish between the personal and professional personas of an employee.
- Social media capabilities are evolving rapidly in both form and volume, straining the ability to capture all the types of data which may be involved including text, graphical, video and audio.

Mitigation

Education: Employees should be made aware of the scope and intent of the policy and how it may affect or interact with existing corporate policies. Such education should be pervasive given that such a policy most likely would affect all employees.

Training: Employees should be provided resources to help them make appropriate decisions when interpreting the social media and related policies. Tools including Frequently Asked Questions (FAQs) and scenarios describing typical scenarios that an employee might relate to are useful in gaining uniform understanding and compliance with policy goals.

Data Retention Tools: Companies should assess their current record retention capabilities to determine their suitability in addressing emerging requirements due to social media use. Such use should cover both the company's use of social media to communicate with and provide services to its customers as well as any communications by associates subject to regulatory retention requirements.

D. Endorsement Guidelines

Description
In October of 2009, the FTC released guidelines concerning the use of endorsements and testimonials in advertising. These guidelines were developed to help advertisers comply with the Federal Trade Commission Act, and require disclosures regarding material connection to the endorser (including, but not limited to: celebrities, bloggers, experts and consumers). In addition, advertisements must only reveal "typical" results and no longer include a safe harbor where the disclosure "Results not typical" is displayed. Both the creators of the ads with endorsements as well as endorsers themselves are made subject to unfair and deceptive claims if the guidelines are not followed. The guidelines establish a duty for endorsers to disclose their relationships with advertisers, even when making endorsements outside the context of traditional ads, such as on talk shows, infomercials or in social media.

Mitigation
Social media provides a rich and interactive environment where both producers and consumers can engage in ongoing dialogue. However, care must be taken when using these conversations in the context of advertising. When using social media to promote a product or service, organizations should consider the following suggestions:

- Bloggers or other online publishers including individuals participating in social media must disclose relationships with advertisers when they receive free products for review, compensation or other consideration. This enables the consumer to better decide how much value to place on the publisher's opinions about the product.
- Company policies and practices should be developed for educating associates, bloggers and other endorsers regarding disclosure requirements. Guidelines around required disclosure format should be included.

Monitoring advertisements for endorsements on key web sites and social media sites should be implemented to ensure proper disclosures have been made.

E. Labor Relations

Description
The use of social media by employees and employers is increasingly being impacted by issues related to employment and labor laws. These issues include pre-employment screening and hiring practices, unfair labor practices, harassment and safety issues. Employers are still struggling to understand how these laws apply to them and their use of social media.

Hiring/Pre-Screening
Social Media has become a useful tool in vetting potential employees. Use of social media for this purpose ultimately puts the employer in the position of obtaining too much and potentially inappropriate/illegal information (e.g., marital status, if the individual has children, ethnic background, age, medical conditions, etc.) about a potential hire. Inappropriate information must not weigh into the hiring decision. However, once obtained, regardless of source, an employee or government agency (e.g., EEOC) could argue that a negative decision was motivated by this information and could lead to further action related to discrimination and privacy violations.

Unfair Labor Practices

Many companies have a policy restricting what employees can post on social media sites and will monitor this activity in an effort to minimize risks associated with inappropriate comments (reputation, violation of regulatory recruitments, damage to the company brand [misrepresentation, leaking of sensitive information, embarrassment, etc.], violations of code of ethics/ company policies, unacceptable statements, etc.). However, employees, unions and the National Labor Relations Board (NLRB) can argue that this restriction is a violation of the National Labor Relations Act and an employee's right to engage in concerted activity (action taken in pursuit of a common goal by multiple employees or by a single employee where the employee is authorized by other employees to act on their behalf). Simply put, an employee posting derogatory and negative remarks about his boss, wages and/or working conditions on Facebook, and his fellow employees responding to these remarks, can be considered concerted activity.

Harassment

Harassment is prohibited under several federal discrimination laws (e.g., Title VII of the Civil Rights Act of 1964, Age Discrimination in Employment Act of 1967 (ADEA)). A harasser can be a boss, co-worker, contractor or client. Typically, harassment usually takes place in the office or at a workplace function. However, harassment can be extended to social media sites also. Employers need to understand that communications through the Internet, email, instant messaging and text messaging can constitute actionable harassment in the workplace, and potentially on an employee's own time.

Safety

Use of social media may even present safety issues that fall under Occupational Safety and Health Administration (OSHA). OSHA has created the "Distracted Driving Initiative." The first area of focus under this initiative is driving while texting. OSHA may issue citations and fines to employers for distracting employees by texting them as they drive. This fine falls under the "general duty" clause under the Occupational Safety and Health Act. This act requires employers to provide a safe workplace free of recognized hazards. Will responding to emails or posting a comment on Facebook via a smart phone be any different?

Mitigation

- One of the most important risk mitigants a company can implement is a clearly posted and well communicated Social Media policy around the usage of social media on and off network and it should:
  - Be narrowly tailored and not overly broad.
  - Balance the employer's need to protect themselves and the employees' right to a personal existence and voice.
  - Reference other related policies, such as code of ethics, Internet usage, Info Security, etc. In addition, any prohibition on disclosure of the employer's confidential, trade secret or proprietary information should be referenced.
  - Contain clear statements concerning employee risks if they do not adhere to these policies. This could include discipline and/or termination.
  - Include a statement of intent to monitor employees.
  - Include clear statement of the fact that employees should have no expectation of privacy when engaging in activities on social media sites on or off network.

  - Explain the risks present in social media and raise awareness to the fact that even seemingly harmless information can reveal too much about the company or people's private lives.
- Carefully consider reason for discipline, and consult with the Legal and Human Resources departments.
- Understand labor laws and maintain a relationship with Legal and Human Resources.
- When vetting potential employees, an employer should:
  - Cleary document the reasons why a person was or was not hired. This should be clearly documented if a potential employee is pre-screened by using social media.
  - Notify potential employees or ask their permission to pre-screen using social media. This should be well documented.
  - If applications for employment are obtained via social media sites, take appropriate measures to ensure there are significant controls in place around these requirements.
  - Train recruiters and hiring mangers on the appropriate uses of social media and EEOC policies.
  - Ensure appropriate separation of duties for recruiters and hiring managers; separate employee performing the social media background check from the hiring "decision makers."
  - Perform periodic audit of recruiting social media sites.
  - Perform periodic independent review of all recruitment methods and tools.
  - Maintain clear documentation for all potential employees.
  - Ensure that the information collected provides insight on the individual's skills or ability to perform the job.
  - Apply a pre-employment policy consistently (screen all or none).
- Verify information obtained on social media – not all information is accurate.
- Companies should review their liability insurance programs, including employment practices coverage, to ensure they are financially covered if they are sued by employees, job prospects or government agencies.

Case Study

American Medical, a unit of "Greenwood Village, Colorado-based Emergency Medical Services Corp., the largest U.S. operator of ambulance services and provider of emergency room doctors," was sued after firing an employee for criticizing her supervisor on Facebook. The case was brought by the U.S. National Labor Relations Board. It was determined that employees have the right to discuss their working conditions even if the Union is not involved. It was found that the employee was "illegally fired and denied union representation." "Among the issues in the case was whether a worker has the right to criticize a boss on a site such as Facebook if co-workers add comments. The case was the first by the NLRB to assert that employers break the law by disciplining workers who post criticisms on social-networking websites." American Medical promised not to deny union representation in the future and that employees won't be threatened with discipline for requesting union representation. In addition, American Medical is updating their overly broad social media policies and guidelines.

F. Payment Card Industry Risk

Description

People posting content to social media sites need to be aware of the rules governing the exposure of card numbers (debit card, credit card) as well as other card-related information such as the cardholder name, expiration date, PIN, security codes (CAV2/CVC2/CVV2/CID) and service code. Exposed cardholder data could lead to the creation of fraudulent transactions or identity theft.

The Payment Card Industry (PCI), composed of the major card vendors (VISA Inc, MasterCard Worldwide, American Express, Discover Financial Services and JCB International), founded an open global forum in 2006 called the PCI Security Standards Council. The Council is responsible for the development, management, education and awareness of a number of Payment Card Security Standards, one of which is the Data Security Standard (PCI DSS). Merchants, processors and issuers for these card brands are required to be compliant with PCI DSS.

PCI DSS contains specific requirements surrounding the display of card data.

- Control 3.3 of PCI DSS version 2.0 states: Mask PAN (primary account number) when displayed (the first six and last four digits are the maximum number of digits to be displayed).
- Control 3.4 of PCI DSS version 2.0 states: Render PAN unreadable anywhere it is stored (including on portable digital media, backup media and in logs) by using any of the following approaches:
  - One-way hashes based on strong cryptography (hash must be of the entire PAN)
  - Truncation (hashing cannot be used to replace the truncated segment of PAN)
  - Index tokens and pads (pads must be securely stored)
  - Strong cryptography with associated key-management processes and procedures.

If cardholder name, service code and/or expiration date are stored, processed or transmitted with the PAN, or are otherwise present in the cardholder data environment, they must be protected in accordance with all PCI DSS requirements *except* Requirements 3.3 and 3.4 which apply only to PAN. Simply stated, the cardholder name, service code and/or expiration date do not need to be made unreadable.

The CAV2/CVC2/CVV2/CID codes and PIN should never be stored or displayed.

Social media sites are not merchants, issuers or processors; therefore, they are under no requirements to maintain the security of cardholder data.

Mitigation

Policies and procedures should include specific controls around posting of card data. In general, the best rule of thumb is to specifically prohibit such posting altogether. If there are specific scenarios that would warrant a reference to a card number, the following direction should be provided:

Debit card account numbers and credit card account numbers must <u>always</u> be truncated or masked, regardless of their association with other data. The first 6 digits and the last 4 digits are the maximum number of digits that can be displayed. Example: "….your card number ending in 1234."

Scenario
A customer uses Twitter to send a tweet to the financial institution about a customer service issue associated with use of his debit card at a particular merchant. In the post, he gives his name, card number, expiration date, merchant name, date of purchase and purchase amount to assist the customer service department with resolution of the issue.

In responding to the issue, the customer service representative should not continue the service conversation with the customer using Twitter other than to direct the customer to a more secure method of communicating with the financial institution about the issue. If necessary, only a reference to the last 4 digits of the card number should be given in the exchange. It would be prudent during a subsequent conversation with the customer to offer guidance and caution regarding the sharing of card data in social media sites.

References
PCI Security Standards Council, https://www.pcisecuritystandards.org/index.php.

G. Marketing Laws and Regulations

Description
Regulators consider websites as advertising, and as such, these sites must comply with various consumer advertisement requirements applicable to the product being promoted, such as Truth in Lending, Truth in Savings, FDIC membership rules, and Unfair and Deceptive Acts or Practices. (For a more comprehensive list of applicable laws and regulations see Appendix B.)

Stronger and more subjective requirements are expected under the Dodd–Frank Wall Street Reform and Consumer Protection Act, especially when it comes to evaluating the fairness of consumer financial products. The current prohibition of unfair and deceptive acts or practices (UDAP) under Regulation AA is expanded under Section 1031 of the Act to include abusive acts or practices. Per Section 1031, "the Bureau may take any action… to prevent a covered person or service provider from committing or engaging in an unfair, deceptive or abusive act or practice … in connection with a consumer financial product or service, or the offering of a consumer financial product or service."

With this new latitude, financial institutions will be expected to comply with the spirit of the law as well as with the letter of the law. This shift is already evidenced in the courts regarding the posting order of items from high to low, which may result in excessive overdraft fees. In 2010, lawsuits against several large financial institutions regarding such practices played out in the media resulting in financial loss as well as reputational damage. Although these practices are not prohibited under the consumer regulations, the court has ruled against the financial institutions, thus indicating that this practice is not in the best interest of the consumer.

In addition to litigation risk, non-compliance with applicable marketing laws and regulations may result in reputation risk, regulatory enforcement actions and in some cases civil money penalties.

Mitigation

The real-time nature of social media, the viral nature of the Internet and the lack of control over content posted in the social media space must be considered during the development of a financial institution's risk strategy. To the extent the financial institution's products and services are being presented, both corporate-sponsored and employee's personal use of social media must comply with applicable laws and regulations. The following elements should be considered for inclusion in the financial institution's risk mitigation strategy to ensure compliance and reduce the potential for reputation risk.

- Perform a risk assessment. Prior to implementing a social media presence, financial institutions should identify and assess the legal, compliance, reputation and operational risks associated with the products and services in scope of the initiative.
- Review content prior to posting. Leverage existing policies, processes and content review procedures related to marketing and advertisement and make appropriate modifications to address the uniqueness of the social media space.
- Establish, socialize and enforce a Corporate Social Media policy addressing personal and corporate use expectations to minimize risk of non-compliance to laws and regulations. (See Reputation Section for more information on employee training and policy guidance.)
- Establish process and accountabilities for ongoing site content monitoring, identification, escalation and remediation of any issues of non-compliance. (See Reputation Section for more information on criteria for reputational threats.)

H. FINRA Requirements

Description

Securities firms doing business in the United States are regulated by the Financial Industry Regulatory Authority (FINRA). Such firms must follow specific regulatory requirements for firm communications with the public that are outlined in NASD Rule 2210, which calls for specific content standards, supervisory review, approval and recordkeeping. Social media activities performed for firm-related businesses are considered a firm communication with the public and must adhere to the same standards as traditional communications, print, television and electronic media. However, this presents a challenge for many firms trying to keep up with new forms of electronic communication methods, including social media and other numerous technologies and systems. Proper supervision and controls are a necessity to ensure that content standards and appropriate systems of record retention are in place.

Mitigation

Proper supervision of firm-related social media should cover the following to mitigate risk:

Static Content

Static content on a social media site is content that has longevity and remains posted until it is changed by the firm or removed. This content typically includes:

- Background profile information (such as a Facebook or LinkedIn profile)
- Disclosures and hyperlinks on the website.

Interactive Content

Interactive content has been regarded by FINRA as a type of "public appearance" which takes place in an interactive forum. This content typically includes:

- Responses to a post or discussion thread (such as a Facebook or blog post)
- Online seminars using unscripted content
- Chat rooms.

Suitability Issues

Securities firms that plan to recommend securities through social media must keep in mind the requirements of NASD Rule 2310 and Notice to Members 01-23 for additional guidance covering online communications and when they fall within the definition of a "recommendation" under Rule 2310.

Under Rule 2310, securities firms are required to determine that a recommendation is suitable for every investor to whom it is made. Many social media sites include functions that make their content widely available or that limit access to one or more individuals, but because of the viral and very public nature of social media, FINRA advises in their Notice 10-06 that firms should consider making it a best practice to prohibit 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. FINRA also notes that firms should consider adopting policies and procedures governing communications that promote specific investment products, even if these communications might not constitute a "recommendation" for purposes of their suitability rule or otherwise.

FINRA also notes that many firms maintain databases of previously approved communications and provide their personnel with routine access to these templates.

Supervision

Social media websites allow for both static and interactive electronic communications as defined above.

Static content is considered an advertisement under NASD Rule 2210 and must be pre-approved by a licensed General Securities Principal of the firm prior to making that content available to the public. The content must be reviewed for appropriate content standards and evidence of this approval must be documented along with the date of the approval.

Interactive content makes up a large percentage of social media and have been regarded by FINRA as a type of "public appearance" taking place in an interactive forum. While public appearances and interactive electronic communications do not require that a registered principal approve the communication prior to use, these communications still require proper supervision to ensure that content standards are being met. This supervision requirement is outlined in NASD Rule 3010.

In FINRA's Regulatory Notice 10-06 it states that firms may adopt supervisory procedures similar to those outlined for electronic correspondence in Regulatory Notice 07-59 (FINRA Guidance Regarding Review and Supervision of Electronic Communications). Firms may employ risk-based principles to determine the extent to which the review of incoming, outgoing and internal electronic communication is necessary for the proper supervision of their business.

The notice goes on to state that firms may adopt procedures that require principal review of some or all interactive electronic communications prior to use. For example, firms may want to include an escalation workflow for subject matter that has significant disclosure and regulatory requirements (such as mutual fund communications) or that may be highly sensitive or controversial. Firms may also adopt a sampling or lexicon-based search methodology as discussed in Regulatory Notice 07-59 for post-use review. For example, a firm's newly launched Facebook page might not have that many fans or interactions on the site resulting in minimal interactions to review. A firm might want to start out sampling a percentage of content on a weekly basis, but then increase the amount and frequency of samplings as more users join the site and as interactions increase.

Internal social media is becoming commonplace at many firms and FINRA's Notice recommends special efforts to adopt policies and procedures to ensure appropriate review of internal electronic communications that require review under FINRA rules and federal securities laws. Rules including NASD 2711(b)(3)(A), for example, require that a firm's legal and compliance department be copied on communications between non-research and research departments concerning the content of a research report.

Reporting of customer complaints under NASD Rule 3070(c) should also be addressed for social media sites that provide channels for customers to interact and post content.

Third-Party Content

For Securities firms that establish a social media presence on such sites as Facebook or other sites that allow third-parties to post content, FINRA has taken the position that they do not treat posts by customers or other third parties as the firm's communication with the public subject to Rule 2210. However, their Notice does state that under certain circumstances, third-party posts may become attributable to the firm if the firm has:

- involved itself in the preparation of the content (the "entanglement theory"). For example, the firm or its personnel paid for or otherwise took part in the preparation of the content, or
- explicitly or implicitly endorsed or approved the content (the "adoption theory"). For example, the firm or its personnel rates a Facebook post with a "like" designation.

Many firms have adopted strategies to help mitigate risk by placing disclaimers on a firm's social media site expressly stating that third-party posts do not reflect the firm's view. In addition, some firms institute use guidelines for third parties interacting on the site, and may block third-party posts or have site administrators screen and remove posts deemed inappropriate.

Recordkeeping

Rules 17a-3 and 17a-4 under the Securities Exchange Act of 1934 and NASD Rule 3110 require that records relating to its "business as such" are retained. This requirement also applies to social media sites conducting firm-related business. Many firms are evaluating outside technology tools that are intended to retain records of communications made through social media sites. However, FINRA cautions in their Notice that it is up to each firm to determine whether any particular technology, system or program provides the retention and retrieval functions necessary to comply with the books and records rules.

Employee's Personal Use

Firms that allow individual employees to set up social media accounts to conduct firm business must have policies and procedures reasonably designed to ensure that these employees are supervised, have the necessary training and background to engage in such activities and do not present undue risks to investors as stated in FINRA's Notice. In addition, firms must have a general policy prohibiting any associated person from engaging in business communications in a social media site not subject to the firm's supervision.

The Notice outlines some considerations when developing policies:

- Prohibiting or placing restrictions on any associated person who has presented compliance risks in the past (particularly compliance risks concerning sales practices).
- Monitoring the extent to which associated persons are complying with the firm's policies.
- Taking disciplinary action if the firm's policies are violated.

Resources

NASD Rule 2210–"Communications with the Public,"
http://finra.complinet.com/en/display/display_main.html?rbid=2403&element_id=3617

NASD Rule 2310–"Recommendations to Customers (Suitability),"
http://finra.complinet.com/en/display/display_main.html?rbid=2403&element_id=3638

NASD 2711(b)(3)(A)–"Research Analysts and Research Reports,"
http://finra.complinet.com/en/display/display_main.html?rbid=2403&element_id=3675

NASD Rule 3010–"Supervision,"
http://finra.complinet.com/en/display/display_main.html?rbid=2403&element_id=3717

FINRA Notice 10-06 Social Media Web Sites–Guidance on Blogs and Social Networking Web Sites,
http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p120779.pdf
FINRA Notice 07-59–Supervision of Electronic Communications,
http://www.finra.org/Industry/Regulation/Notices/2007/P037553

FINRA Guide to the Internet for Registered Representatives,
http://www.finra.org/Industry/Issues/Advertising/p006118

FINRA Podcast–Electronic Communications: Social Networking Websites,
http://www.accelacomm.com/jump/podcast_127/www.accelacast.com/programs/FINRA_podcasts/FINRA_Podcast_Elec_Comm_Social_Networking.mp3

FINRA Podcast–Electronic Communications: Blogs, Bulletin Boards and Chat Rooms,
http://www.accelacomm.com/jump/podcast_125/www.accelacast.com/programs/FINRA_podcasts/FINRA_Podcast_Blogs_Bulletin_Boards_Chat_Rooms.mp3

FINRA Podcast–Electronic Communications: Websites,
http://www.accelacomm.com/jump/podcast_123/www.accelacast.com/programs/FINRA_podcasts/FINRA_Podcast_Elec_Comm_Web_Sites.mp3

SEC Interpretation–Use of Electronic Media, http://www.sec.gov/rules/concept/33-7288.txt

SEC Interpretation–Guidance on the Use of Company Websites,
http://www.sec.gov/rules/interp/2008/34-58288.pdf

FINRA–Electronic Communications Advertising Regulation Conference October 21-22, 2009, Washington, DC,
http://www.finra.org/web/groups/industry/@ip/@edu/documents/education/p120155.pdf

FTC's Guides Concerning the Use of Endorsements and Testimonials in Advertising,
http://www.ftc.gov/opa/2009/10/endortest.shtm

II. LEGAL

A. Lack of Separation of Personal and Professional Communications

Description
When employees use social media for both personal and professional purposes, there is greater risk of mistakenly using work-related accounts to express personal opinions or of accidently communicating with personal contacts through a work account. Compounding this confusion are the evolving terms of service of various social media platforms, such as Facebook, which allows a person to create an official company page for his or her business but requires they use the same personal email account assigned to the their personal page. This ambiguity can create a great deal of confusion that could expose the company to reputational, legal and other risks.

Mitigation
Employees who are assigned responsibility to manage a corporate presence on a platform either through a personal account or professional account need to be sure they can distinguish between business and personal communications. In consultation with company compliance and legal teams, employees can avoid such risk in a variety of ways, including:

- Only read and respond to messages, alerts or postings from the specific webpage to which they are attached. This will greatly reduce the risk that the employee uses the wrong account by mistake (as can happen from a mobile device).
- Ensure that a business account, while it is linked to a personal account, has notices forwarded to a work-related email, or in the event of mobile messaging, that personal and business alerts are directed to separate cell numbers.
- Only link work-related accounts to the same third-party platform (such as HootSuite) on business and personal computers and mobile device applications. By using two different such platforms (one for each type of account) users will sharply reduce confusion between personal and professional communications.
- Attach a boilerplate disclaimer to personal messages that stipulate that the views expressed do not reflect those of the company (although this solution may not be enough to mitigate reputation risk should the user "speak" from the wrong account).
- Make it company practice to:
  - conduct all work-related social media contacts at work and on company equipment.
  - draft all social media messaging in a word processor so the message can be carefully reviewed and so the employee can check that the right account is being used before transmitting.

Scenario 1
A user has a personal account and then creates an account for business purposes with the same email, in accordance with Facebook's terms of service:

Maintaining multiple accounts, regardless of the purpose, is a violation of Facebook's Terms of Use. If you already have a personal account, then we cannot allow you to create business accounts for any reason. You can manage all the Pages and Socials Ads that you create on your personal account.

This means that when new postings are attached to the "wall" of Facebook pages, alerts about new messages on both the business-related and personal pages will appear in the same email account or on the same PDA such as a BlackBerry. With the commingling of alerts a user could accidentally respond to the posting (or worse yet tweet a reply or comment) through the wrong account and therefore to the wrong audience.

Scenario 2
Huffington Post, March 10, 2011:

SAN FRANCISCO — Chrysler Group LLC is ending its relationship with the social media agency that was behind an obscene tweet that was posted to the Chrysler brand's official Twitter account.

The tweet was posted Wednesday by an employee of the company's agency, New Media Strategies. It read: "I find it ironic that Detroit is known as the #motorcity and yet no one here knows how to (expletive) drive." Shortly after, the tweet was removed from Chrysler's Twitter feed….

… Chrysler said in a follow-up post Thursday that the tweet "obviously" was meant to appear on the employee's personal Twitter account, rather than on Chrysler's, and that automaker did not demand that person be fired.

Worker Fired for F-Bomb Tweet on Chrysler Twitter Account,
http://www.huffingtonpost.com/2011/03/10/chrysler-twitter-f-bomb-tweet_n_834246.html

B. Civil Litigation

Description
Social Media greatly increases the ability for employees to open their firm up to the risk of lawsuits by their actions. When an employee acts as a representative of their firm or provides a direct association, their actions could potentially be used against the firm. Examples may include an employee blogging about a current court case; an employee discussing client information or providing client sensitive data; an employee inadvertently allowing their network to be infected with malware (See Spreading Malware Section) that could impact clients' sensitive data; and more.

Mitigation
As with any other risk resulting in harm to the employee's firm, strong policies and procedures outlining the use of social media both professionally and personally reduce civil litigation risks. Employees should be fully trained on proper usage and understand all policies, procedures and consequences for failing to comply.

Scenario 1
An employee has a personal account that lists their employer and perhaps other information relating to the firm such as their position or department. The employee makes claims that may be construed as on behalf of his/ her employer that result in litigation against the firm, negative and unwanted publicity, and lead to brand degradation and or loss of shareholder trust and confidence. (Please also refer to Reputation Section.)

Scenario 2
A user does not set the privacy settings adequately to block viewing by unauthorized persons. Law enforcement agencies, creditors, opposing counsel, or others mine the site for discovery purposes resulting in legal action or embarrassment to the user. If the user indicates his/ her employer on the page any resulting negative or harmful publicity or actions may reflect poorly on the firm.

C. eDiscovery

Description
Legal discovery is the act of locating all documents that are relevant to support litigation. Similarly, eDiscovery involves locating Electronically Stored Information (ESI) for the same purpose. Information on social media sites falls under the category of ESI. There are several aspects of legal discovery, including preservation, privacy and admissibility, which impacts eDiscovery and potentially leads to risks associated with the use of social media.

<u>Preservation</u>
Preservation of information includes the storage and retention of information in a way that maintains its integrity and prevents unauthorized access, modification and destruction.

Several challenges exist regarding the preservation of information on social media sites:

- Because information on social media sites is stored outside a business' firewall by a third party, it is not owned or controlled by the business. This can present a challenge to retrieving and accessing this information. Social media sites have their own retention policies, which determine what information is retained, the retention period for that information, and how it is protected.

- Businesses may also be faced with the challenge of litigation hold requirements for information that is stored on social media sites. When litigation is pending, the business must ensure relevant information is not purged after the appropriate retention period, until notified by the attorney of record that the case has been resolved. This burden is placed on the business. However, it is unclear if the same legal requirement applies to the social media site on which the information may be stored.

- It is possible for businesses to capture information stored on social media sites. However, the amount of information to retrieve and store, who retrieves this information (e.g., third party), and the frequency at which the information is captured (static vs. dynamic) can have a significant impact on resources and costs. Furthermore, keeping too much information can also be a legal issue. Until information is purged, it is discoverable. This includes information that exists beyond the required retention period.

Privacy

Privacy, specifically the expectation of privacy, can be impacted by:

- The ability to instantly share with many different individuals across the globe.
- Each individual's privacy settings and diligence therein.
- Private communities set up by users on a social media site.
- The terms and agreements and communications by the social media site on the expectation of privacy. Depending on how the expectation of privacy is perceived and defined will determine whether or not information is available for eDiscovery purposes.

Admissibility

Admissibility is the acceptance of information as evidence. One of the major factors affecting admissibility is the authenticity of the information, which can be questionable since information on social media sites is susceptible to manipulation or fraud due to spam, hackers, viruses, etc. Minimizing this susceptibility relies heavily on the controls put in place by the social media site.

Mitigation

Obtaining information from social media sites can be difficult and costly. Rules and requirements around this topic are evolving and so are the risks. Suggestions for minimizing risks associated with eDiscovery include:

- Set policies on the use of social media sites and the use and preservation of information, including information on social media sites. Communicate to and train employees on these policies and the risks of using social media.
- Establish an information retention program, and document gaps and plans for remediation. Use the same principles for social media sites.
- Take inventory of social media sites used by your organization. Research and understand the controls and policies set by these social media sites.
- Look into software that is available for the preservation and production of social media information.
- Make your best effort. Maintain consistency with retention and discovery practices, and demonstrate logic in decisions made regarding these practices.

References

National Law Review Blog, http://www.natlawreview.com

K&L Gates Blog on issues related to eDiscovery, http://www.ediscoverylaw.com

ARMA International, not-for-profit professional association specializing in records and information management, http://www.arma.org/

General Counsel Roundtable, https://gcr.executiveboard.com/Members/Default.aspx

Relevant Laws
eDiscovery Amendment to the Federal Rules of Civil Procedure – introduces the phrase "electronically stored information" and the ability to, along with the issues of, using this information in the discovery process.

Stored Communications Act. Addresses privacy issues for stored electronic information on the Internet, http://www.justice.gov/criminal/cybercrime/ssmanual/03ssma.pdf.

Rules of Evidence. Governs the admissibility of evidence, http://www.law.cornell.edu/rules/fre/rules.htm.

III. OPERATIONAL

A. Identity Theft

Description
According to the Identity Theft Assistance Center (ITAC), "Social networks like Facebook are a great way to share information that's important to you. Unfortunately, they are fertile ground for criminals looking for information that can be used to commit identity theft. A study by Consumer Reports found that 52 percent of social-network users post their full birth date, home addresses, vacation plans or other personal information that could increase their risk of becoming victims of identity theft or other computer crimes."

Most authentication methods in use today include the use of shared secrets, which is generally comprised of information available from public records as well as out of wallet information such as name of oldest nephew, date of birth, name of pet, schools attended, etc. In many cases, this information can be acquired from information shared in posts, photos and profiles published on social media sites.

The user's ability, or inability, to control access to the information posted on the social media site has been a source of controversy and criticism in the media. The lack of transparency on the part of the social media service provider on what information is being shared and with whom, a lack of user controls to provision access to their posts, as well as misconfigured privacy settings can all expose users to unintentional sharing of personal information which may enable hackers to obtain answers to standard security challenge questions.

While the concentration of media attention has been focused on personal risks associated with personal use of social media, hackers have also targeted personal and corporate information available within social media channels to obtain information later used to exploit employee credentials and breach corporate security.

During the 2010 DEF CON Hacker Conference, DEF CON hosted a Capture The Flag (CTF) contest that tested participants' social engineering skills by requiring participants to legally social engineer their way into a target company. Social-Engineer.org published the contest results in a report entitled "Social Engineering Capture the Flag Results DEF CON 18" on their website. The report states that the "use of public social media resources to attack organizational assets is a common issue in real world attacks, a fact that was reflected in this event."

The report indicated that contestants were able to obtain a significant amount of information to develop dossiers on their targets through various social media channels. "The use of Google, Google Earth and Google StreetView provided an amazing amount of information for the contestants. Also used were social media sites such as Facebook, MySpace and LinkedIn. While Facebook, MySpace and similar sites have garnered the most attention by the media, it was LinkedIn that provided the most information, in a few cases providing the contestants with the ability to develop an organization chart for the target."

Corporate and employee presence in social media may directly or indirectly expose the organization to identity theft or information breaches resulting in identity theft.

- Corporate profiles can provide useful information to facilitate social engineering attacks against the organization.
- Information shared or contained within an employee's personal or professional profile may provide tips for guessing user ids or passwords for access into the corporation's internal applications or systems.
- This same information may provide answers to security challenge questions.

Mitigation

ITAC has a wealth of information to help consumers avoid becoming victims of identity theft, which includes the following tips for social media use.

- Think about keeping some control over the information you post. Consider restricting access to your page to a select group of people, for example, your friends from school, your club, your team, your community groups, or your family.
- Keep your information to yourself. Don't post your full name, social security number, address, phone number, or bank and credit card account numbers — and don't post other people's information either. Be cautious about posting information that could be used to identify you or locate you offline. This could include the name of your school, sports team, clubs, and where you work or hang out.
- Make sure your screen name doesn't say too much about you. Don't use your name, your age, or your hometown. Even if you think your screen name makes you anonymous, it doesn't take a genius to combine clues to figure out who you are and where you can be found.
- Beware of phishing attempts. It can be hard to tell if an email supposedly from a social networking site you belong to is an attempt to steal your login information. To be safe, never click on a link from an email that looks like it came from a social networking site–type in the site's URL manually.
- Don't be scammed. Scammers can gain access to one of your friend's accounts and then solicit all the friends linked to the account for money. Never respond with a credit card number or online payment, even if it looks like it is from a friend. Call your friend and ask if it's a legitimate request.
- Choose your password carefully. Make it at least eight characters and include a number and a symbol in it. This way it's very difficult for someone to guess your password and hijack your account.

Additionally, using the same user id and password for multiple sites increases your exposure if credentials are compromised. Ideally, users should select unique user ids and passwords for each site accessed to minimize that risk.

The DEF CON report provides the following warning and recommendations to corporations related to the use of social media. "The threat that social engineering poses to Corporate America must be taken seriously. The big challenge for any organization looking to defend itself from this threat will be to find a balance between their customer-centered training and their anti-social-engineer security training. Companies want to help their customers, but they don't want to sink their ship by sharing seemingly trivial information. Savvy organizations have found that the best prevention naturally falls into place when they identify any security training gaps, include all employees in their security training program, and distribute anti-social-engineer tips on a regular basis."

Financial institutions should consider the following measures to mitigate id theft risk.

- Establish a social media use policy and best practices.
- Raise awareness through training and communications.
- Monitor for compliance with corporate policy and address policy exceptions as appropriate.
- Monitor use of corporate brand on the Internet.
- Modify security challenge questions to eliminate or place less emphasis on information that may be readily available on social media sites.
- Require unique and complex passwords for access to systems containing confidential customer or corporate information.
- Consider a cyber liability policy to provide full limits for notification, remediation, forensics and potential coverage for fines and penalties due to customer financial data intentionally being leaked by an employee or customer.

B. Spreading Malware

Description

Malware, short for malicious software, is software designed to harm a computer system without the owner's consent or knowledge. The software is considered to be malware based on the perceived intent of the creator, not its particular features. The software code includes viruses, worms and Trojan horses. Malware will utilize popular communication tools, such as worms through emails and instant messages, Trojan horses from websites and virus-infected downloaded files shared from peer to peer connections. The software seeks to exploit existing vulnerabilities, flaws in computer software that create weaknesses, on systems making their entry easy and discreet.

According to a report published by Sophos in 2010, malware is on the rise on social networks such as Facebook, Twitter, LinkedIn and MySpace. In the past year, 36% of users reported being sent malware via social networking site, an increase of 70% from the previous year. Sophos surveyed more than 500 organizations with 72% thinking social networks are a danger to the company. Sixty percent of the organizations stated that Facebook was the biggest security risk, followed by MySpace, Twitter and LinkedIn.

Malware spread through social networks is a security risk to financial institutions due to:

- Potentially increasing threats of malware attacks to the institution's infrastructure and data due to employee use of social networks on company property and through remote access devices.
- Threatening the consumers' trust in the institution's security measures and handling of their personal and financial information.

Mitigation
Social networks have become an essential part of the business mix, so institutions cannot just block access to them. Instead institutions need to apply security measures, educate employees and customers, and implement training, policies and procedures to mitigate the risk.

Institutions can:

- Use a third-party vendor to monitor IT infrastructures, scan all files downloaded and keep security patches up to date.
- Make sure employees use effective passwords and multifactor authentication technology.
- Enforce security policies and procedures.
- Prohibit employees from installing unauthorized software.
- Deploy an automated backup software to safeguard data.
- Utilize full-disk encryption software to render hard drive data illegible to anyone that doesn't have proper authorization.
- Use of key fobs to log in to a secure network from an unsecure access when employees work remotely.
- Monitor website traffic and restrict access to sites that pose significant risk.
- Have an emergency communication and response plan.
- Implement a security awareness program to educate employees on the risk of using social networks, especially those with social network access.
- Have a social media disclosure that advises customers not to click on links posted by other users and warn that it may pose risk to their computer.
- Create and consistently use a unique shortened URL so that customers recognize your institution's links and know that they can be trusted.

C. Social Engineering

Description
Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information, namely the unauthorized acquisition of sensitive information or inappropriate access privileges by a potential threat source. The term typically applies to exploitation of trust or building of an inappropriate trust relationship with a legitimate user, the creation or exploitation of confidence or vanity to gather information or influence the actions of another individual or entity for information gathering or computer system access.

The goal of social engineering is to *trick someone* into providing information they would not otherwise share or divulge. Commonly used social engineering techniques include:

- Pretexting
- Phishing or SMiSHing
- Pharming
- Vishing or Phone Phishing.

Mitigation
Social engineering is proliferating and evolving so rapidly that standard security policies, operational procedures and technical solutions cannot adequately protect financial service institutions. Creating a security aware culture requires the active commitment and accountability of everyone, from the Board to every employee, contractor and vendor.

Continual education and awareness is key to coaching employees to heightened awareness of sophisticated social engineering exploits and tactics. Depending on the accepted or anticipated extent of usage of social media channels by employees, contractors and/or clients, training should be as specific as possible to the potential exploits of social engineers and does not mean blocking social media from financial institutions.

A security aware culture includes:

Security Awareness Training
The best way to avoid unintentional security problems is to provide all employees with frequent security awareness training specific to social media. The training should be used as a venue to inform employees of new threats as well as a refresher on how to identify and avoid social engineering attacks. The training program should focus on potential areas of exploitation, whether that is by job function, type of technology, increased momentum of social engineering ploys in certain channels, and/or shift of types of attacks or exploits.

Most employees do not cause security problems intentionally. Accessing unsecure websites, deploying unauthorized wireless access points, or falling victim to social-engineering ploys are common employee actions that may result in security breaches.

An annual seminar or occasional memo is not an effective approach and is not recommended. Organizations must treat security awareness training as a continual, enduring aspect of employment.

Policy and Awareness
Information Security organizations should set the tone for an institution's policy and awareness for actionable intelligence with social engineering and social media channels. This should be in collaboration with the institution's regulatory, legal, supply chain and technology organizations and may include such specifics as password lengths, numbers and type of characters that each password must include; how often a password must be changed; current software versions; formal assessment and classification of the value of information being sought with recommendations for prioritizing and protecting it (logical and physical); and inclusion of social engineering information in an institution's Social Media Policy and Guidelines.

The technical mitigation and detection of social engineering includes:

- Detection comes in several forms, but relies mainly on associates being skeptical of unusual requests. Employee monitoring, requests for change in the level of access, and other insider threat related concerns are essential to helping pinpoint possible social engineering attempts. Detection as a social engineering attempt is occurring is difficult, though there are measures that can be implemented to ensure associate identity, such as having a multifactor authenticator in place for such occasions.

- Deploy an intelligent web proxy to block certain functionality on social media sites identified as risky. For example, access to a particular site could be enabled, but the ability to run applications, post or access other expanded functionality on that site would be blocked by the web proxy.

- Deploy a DLP (Data Loss Prevention) solution on web traffic to block information classified as sensitive or high risk. This would provide the ability to identify and filter sensitive information that is posted through web channels. This ability could involve simple filtering and alerting on key words or the active blocking of traffic from specific hosts based on dynamic criteria and the density of sensitive information in a post. This solution would be significantly more effective if the SSL stream were broken to allow inspection, but that is not necessary for basic function. This solution could be integrated with the web proxy mentioned above.

- Deploy a DLP solution and content blocking on corporate email to identify spearphishing attacks. Desired capabilities would include the ability to identify and filter outbound emails that contain sensitive information, especially to sites or domains that are not appropriate recipients of such information, such as gmail.com or hotmail.com addresses.

- Assessment on social media platforms similar to vendor assessments of critical suppliers should be considered. Employees should be made aware of the various restrictions and security measures that may be used on popular social media websites. Given high instances of usage by employees of all sites in question, an internal assessment of security should be made. Those employees who are at higher risk for social engineering should be investigated, where possible, for potential information leaks on their personal pages; steps should be taken where necessary to ensure proper education regarding information disclosure and education of the associate about the potential for harm caused by revealing too much information publically.

Scenarios

Scenarios using various techniques available in a social engineer's tool kit include:

- <u>Spearfishing:</u> Using information gathered from a passive source, a social engineer could create an identity designed to attract the interest of specific targets. The attacker can then engage and interact with contacts and actively harvest information while protected by the layer of anonymity provided by electronic communications.

- <u>Enumeration:</u> An employee user posts their resume showing extensive, current experience with a specific product or technology, potentially giving attacker valuable information to target their attack. The same employee could post a comment about having to work overtime, and provide sensitive details regarding why. <u>This is more passive than active social engineering.</u>

- <u>Malware Propagation through Transitive Trust:</u> As in the case of an email virus, one user triggers malware, such as a clicking on a link and executing a program that sends a link to a compromised site to all users they associate with on a particular social networking site. Since the link appears to be coming from a known friend or associate the recipients are more likely to click on the link and be compromised, spreading the malware to more users.

- <u>Application Posting:</u> Facebook applications can post links in a user's name without the user's consent after initial approval. This may allow the owner of the application to influence the user's contacts through the veil of the personal relationships already established.

- <u>Blackmail:</u> A user reveals personally or professionally sensitive information on a social networking site. The social engineer engages and encourages them to say more, then threatens to publicize the sensitive information unless the user provides other information or services.

D. Disclosure of Intellectual Property or Other Sensitive Information

Description
As described throughout this guide, social networks/social media are all about sharing. Unfortunately, users of social media can advertently or inadvertently share information that is considered sensitive or proprietary from a business perspective.

This risk entails accidental or intentional disclosure of company secrets, strategies or other proprietary and possibly patented information via a social media site, as well as private information about clients or other outside users and stakeholders. This could include:

- secret formulas (such as the recent publicity surrounding Coca-Cola's recipe)
- programming code
- strategies for marketing, business development or acquisitions
- client information: credit card or social security numbers, birthdates, addresses, etc.
- any type of disclosure that may put the company at a competitive disadvantage or could expose individuals to risk of identity theft or invasion of privacy.

Such situations put a company at risk of civil legal action surrounding the failure to protect such data, regulatory penalties and even loss of reputation and a damaged brand.

Mitigation
All company employees and contractors should be thoroughly trained on what information about their jobs, the company, their co-workers, clients or vendors may be shared either through corporate accounts or their own. An external social media policy and guidelines, as well as a code of conduct addressing social media communications can help employees avoid unintentionally divulging proprietary or confidential information.

Consideration should be given to the creation of two sets of policies – one governing personal usage by employees and the other governing business usage. With regard to employee usage, the following guidelines should be considered when developing policies and procedures:

- Employees are expected to comport themselves professionally when using social media. That means not posting items or saying things on social media which might be considered proprietary or sensitive corporate information or could be looked upon as disparaging to the company or to others whether inside or outside the company.
- Company policies must be adhered to, one example being not disclosing any non-public financial or operational information.
- Make it clear that the use of company computers or networks to access social media is subject to review by the company and that there is no expectation of privacy when utilizing these computers or networks. It should also be made clear that misuse could be grounds for disciplinary action including termination.
- Create a mechanism for reporting any violations of company policy that occur through the use of social media.
- Designate a manager that has oversight over the use of social media that has the responsibility to review all reported violations.

With regard to business use where the use of social networks is part of a person's job, consideration should be given to following policies and procedures:

- Making training on the use of social networks mandatory. Thought should be given to providing guidance on protecting the company's proprietary or sensitive information, Internet etiquette, the proper and approved use of wikis, threads and blogs, and the protection of the company's reputation. Make sure that employees understand that they have no expectation of privacy with regard to the expression of views, opinions, or opinions regarding the company's business and that any views expressed should be clearly identified as being their own.
- Informing employees of the permitted use of logos, trademarks and brands when transacting business on social networks.
- Providing employee training that spells out what should or should not be shared when utilizing social networks and making certain that they understand how they can be exploited through social engineering when on a social networking site. Social engineering can take many forms but some of the more typical ways to exploit a user are:
    - Stealing passwords by utilizing profile information to guess a victim's answer to a password reminder question that allows them to set up another password in the victim's username.
    - A hacker gains the trust of the victim by friending the person on a social networking site and getting them to click on links that contain malware that can then exploit the company's network.
    - Impersonating someone that the victim knows and then asking the victim to do them a favor like providing certain company information (like a spreadsheet or other data) that can then be exploited.
    - Impersonating an insider and looking to gain access to company information.

- Providing employees with useful information on how to avoid sites that may present security risks.
- If you are a public company, making sure employees understand what they can and cannot say for regulatory purposes, e.g., SEC Regulation FD in the case of public companies.

But, policies and procedures and good compliance oversight are only part of the equation for addressing the risks inherent in the use of social media when dealing with sensitive or proprietary corporate information. Collaboration with your IT department is essential to addressing the vulnerabilities that exist in this regard when using social networks. The ways in which companies can address these vulnerabilities from an IT perspective are as follows:

- Making sure that firewalls and intrusion detection and/or intrusion prevention systems are in place and kept up to date and actively tested.
- Implementing data loss prevention tools that block the sharing of regulated or sensitive content as identified by the company on certain social media or third party sites, e.g., sites that present reputational or security risks or access to personal email addresses such as g-mail, aol, msn, yahoo, etc.
- Encrypting or tokenizing data that is placed on social networking sites, particularly collaboration sites.
- Utilizing web monitoring tools that prevent access to sites that pose security risks.
- Installing review tools that allow for monitoring of posted content.
- Employing identity management tools so that the identity of everyone accessing social media sites can be tracked.

Above all, encourage the use of good common sense and judgment. Remember that social media communication by an employee may be reviewed, copied and disseminated by others, including competitors. Good judgment should also lead employees to understand that statements or disclosures that violate the privacy, trade secret, intellectual property or other proprietary rights of any individual or organization are inappropriate and may have legal and reputational implications including but not limited to termination of employment. Employees must show the same respect for sensitive or proprietary information as they would want for themselves.

Preventing intentional information leaks is more problematic; even companies that strictly limit social media access to a select group of employees may fall victim to an employee's deliberate and malicious disclosure of company information. In such cases, which are rare, vigilant use of various technology tools for monitoring of content and the robust crisis communications plan can reduce the negative impact of such information leaks.

Scenario 1
A software developer posts to a forum or blog regarding his work on a revolutionary new customer application from the company. The developer reveals too much about his product development, thereby enabling a competitor to steal the idea and get to market sooner with a similar application.

Scenario 2
A marketing manager tips off Facebook friends of several successes in winning new business and mentions the new clients joining the firm. Such information violates client confidentiality and puts

the company at great reputational risk (especially among clients and prospective clients), which ultimately could impede the accomplishment of business goals.

E. Products Lack Maturity

Description
Social media is relatively new to the marketing industry and according to the Econsultancy Social Media and Online PR Report 2010, 5% of companies don't do anything, 40% have experimented with social media but have not done much, 36% do an average amount and 18% are heavily involved in social media. One reason why so few companies are heavily involved in social media is that it is not yet mature. Social media products not being mature presents potentially serious consequences to financial institutions that can affect brand image, security reputation, the bottom line and customers' personal and account information.

In 2010, Facebook and Twitter were the social networking sites most affected by security breaches. The sites have become the ideal environment for cybercriminals due to users of these sites placing more trust in them than other sites. This presents a serious risk for financial institutions and the safekeeping of their customers' personal and account information and the company's image should the business account be compromised.

One way social media sites are not mature is through account access and access to analytical data. The sites have not evolved, or advanced, to provide organizations the types of account set up, access and control necessary, nor the analytical data desired. Currently, social networking sites are connected to personal accounts, only offer one credential to access the account and provide limited to zero analytical data to analyze and report back to management on the initiative's success.

Financial institutions should also be aware that due to social media products not being mature, they are constantly changing which can be positive, and negative. Staying updated on all of the site updates requires a significant amount of attention and time to stay aware of what potential changes may impact internal processes and procedures and help the organization remain competitive in the social media space.

Mitigation
The immaturity of social media products is a risk to any organization, thus explaining why 45% of companies either don't do anything or have only experimented with social media. This is especially precarious for financial institutions due to the type of data that may be compromised and how it may affect the brand image and customers' perception of the company's security measures. However, there are actions that can be put into place and tools to help mitigate this risk.

First, create a policy and guidelines for the overall organization regarding social media and the specific individual, or team, that have will be accessing the company social media profiles.

To reduce potential account security risks an organization can limit access to only select individuals. Another option is to use a free or fee-based tool, such as Radian6 Engagement Console and HootSuite, which will allow multiple employees to have access to the profiles and assign and monitor tasks. With these tools, each individual will have their own credentials, while the primary company profile account will remain secure and can be updated to remove rights should something happen.

Post social media disclosures on your profiles and company site advising customers that your organization will never ask for personal or account information, that the company is not affiliated or responsible for the security, privacy or any other operations of social media sites, and that the company reserves the right to remove posts that are inappropriate. Include information on how to contact the company should they have a question, issue to report, or complaint and the customer does not want to post it on that specific site.

Assign the social media team to actively manage company profiles and keywords for suspicious activity with the use of free or fee-based social media monitoring (See Monitoring for list of available tools). Select suspicious activity can include:

- Facebook:
  - Posts by other fans that direct customers to another site.
  - Messages sent to members requesting account information.
  - Discussion posts requesting account information.
  - Posts by users that include personal or account information.

- Twitter:
  - Tweets by other users about the brand with links to suspicious sites.
  - Retweets of company tweets with suspicious activities.
  - Tweets on actual company profile.
  - Tweet, replies or direct messages by users that include personal or account information.

- Community/Forums:
  - Posts by users that direct customers to another site.
  - Posts requesting account information.
  - Posts by users that include personal or account information.

Develop a strategy to manually log and measure social media measurements, or find sites that provide some analytical data. Facebook and LinkedIn provide comprehensive insights for Facebook Pages and company pages, but Twitter and several other sites currently do not so those will have to be handled differently.

Lastly, create a social media workflow for yourself or your team to help you optimize and manage time when researching new social media announcements and upcoming site updates. Setting aside dedicated time for this will help create clear goals for all tasks and set up milestones to help ensure that time is efficiently allotted to all important tasks too.

References

Social Media and Online PR Report by Econsultancy, September 2010, http://econsultancy.com/us/reports/social-media-and-online-pr-report

Facebook and Twitter Most Unsafe Social Networking Sites in 2010, http://www.socialtimes.com/2011/01/report-facebook-and-twitter-most-unsafe-social-networking-sites-in-2010/

Stalking Victimization in the United States,
http://www.ncvc.org/src/main.aspx?dbID=DB_SocialNetworkingSites932

F. Managing Access

With so many legal issues and security threats related to social media use, it's important that financial institutions carefully manage employee access to social media sites. Restricting social media access to only those employees that have a legitimate business need will make monitoring much easier. This practice helps ensure that social media sites are only used for business, and the employees with access have been properly trained on all company social media policies. These policies are put in place to protect the company from unwanted risks.

Some risks of uncontrolled access to social media include:

- Reputational risk.
- Information security and fraud risks (social engineering and phishing that can result in data and identify theft, malware attacks from hackers and spammers, and leaking of proprietary and confidential company information).
- Liability for an employee's negative statements about another person or competitor on a website or blog.
- Disclosure of confidential information, trade secrets or intellectual property infringement by an employee.
- Charges of securities fraud arising from material misrepresentations posted by employee.
- Lawsuits over employee language or activity that is harassing, discriminatory, threatening or derogatory.
- Loss of employee productivity. According to Time Management News, employees who access Facebook, Twitter or other social media sites during office hours waste approximately fifteen minutes to two hours every day. This results in an institution-wide drop in total worker productivity of 1.5%. A survey completed by Nucleus Research revealed that only 13% of the employees that report accessing social media during work hours could identify a business reason for doing so, thus the majority of employees accessed it for personal reasons.

Mitigation

- Access Controls
  - Limiting access to social media sites to only those individuals who have legitimate business needs and who have gained formal approval to use such sites.
  - Permitting employees to access social media sites only during lunch breaks under certain conditions, such as prohibiting the downloading of materials from social media sites and linking to other sites from shortened URLs.
- Formal Policies/ Guidelines:
  - Policies and guidelines should be implemented institution-wide to ensure that all employees understand the expectations regarding their comments about the company either at work or in personal social media use outside of work. Also, current electronic

communication and media relations policies should be updated to include social media sites.

- Monitoring:
  - Human Resources, Compliance, Information Security and/or the social media administrators should monitor mentions of the company with the use of free or fee-based tools.
- Training and Communication:
  - Develop training to educate employees on the policies, expectations of them, and the potential company risks social media presents.

References
Social Networking Impairs Workplace Productivity, http://www.timemanagement.com/news/social-networking-impairs-workplace-productivity.html

Facebook: Measuring the Cost to Business of Social Networking, http://nucleusresearch.com/research/notes-and-reports/facebook-measuring-the-cost-to-business-of-social-notworking/

G. Measuring Success

Description
Calculating a social media return on investment (ROI) presents a challenge. Institutions and marketers realize the potential and importance of communicating and connecting with consumers through social media channels, but justifying the dollar and time investment is problematic. Unfortunately, there is no one-size-fits all methodology for financial institutions and the standard ROI calculation just does not apply. As of August 2010, 56% of marketers were unable to quantify the effect of social media based on a survey conducted by Aberdeen Group. In addition, the "State of Social Media 2010" report, by Smartbrief, Inc. and Summus Limited, stated that less that 15% of businesses using social media are measuring ROI, over 33% are not measuring it at all, and the remaining 52% measure ROI somewhat or don't know if is measured.

Mitigation
There are some metrics that can help gauge the effectiveness of social media efforts until a reliable and widely accepted practice emerges. An array of current tools includes offerings from Facebook, Google, bit.ly and YouTube, to formal fee-based monitoring and analytical tools, such as Radian6, which provides data that can be analyzed in determining success. For any of these tools to be useful, the first step for an institution is to determine its objectives for social media use, what it wants to measure and how. It's advisable that a company be selective in the metrics it uses. A common mistake is to make data collection and analysis time consuming and overwhelming. It is better to track only those metrics that support the objectives. These metrics have been broken into three categories:

- Exposure: Includes metrics that quantify social media efforts. Exposure metrics are most closely related to business performance objectives.
- Engagement: Includes interaction-related metrics. Engagement metrics are closely related to brand and communication objectives and directly correlated to exposure metrics.

- Outcomes: Includes metrics that quantify the outcome of social media activity and, when possible ROI. Outcome metrics are most closely related to business success objectives.

Exposure

- Traffic: Traffic metrics measure effectiveness in creating exposure to a social media profile, material and messages. The metrics can include the number of likes on Facebook, followers and lists on Twitter, channel views on YouTube and subscribers to a blog. Some measure the number of clicks and downloads to a new whitepaper after promoting it on Facebook and the number of times website content is shared via Like, Tweet and in Share.

- Search Ranking: Major search engines count links as if they are votes to a site, and several companies use this metric to gauge the impact of their messaging.

- Referrals: It is closely related to Search Ranking, measuring referrals will reveal whether your social media efforts are successful, and if you are creating enough exposure and posting interesting content (a good example is the "retweeting" of an original tweet, thereby expanding its reach exponentially). Such referrals indicate the success of social media while also permitting a company to follow the reach of its content.

- Leads: For both B2B and B2C objectives, leads are effective way to measure your social media exposure. How it is measured depends on the systems in place, whether it be completing an online form to request more information, a whitepaper or application downloads, or new online applicants.

- Applicants: If one social media objective includes recruiting, the number of applications received is a direct measure of success in creating brand awareness and exposure. It can also be extended to include the number of interviews held, time required to fill a position, and reduced recruiting costs.

- Registrations: Tracking and measuring user registrations for access to company whitepapers or other downloads, enrollment in company webinars, email opt-ins, and RSS feed subscriptions are also effective in tracking the success of your social media initiatives with existing customers.

Engagement

- Interactions: Participation is an indicator to measure the success of your social media efforts and includes the number of comments and replies, participation in communities, reviews and rates, and forum discussions. Interactions can occur on a company website and branded profiles, or on third-party websites.

- Engagement: Engagement metrics include: number of profile views; number of fans, followers, and subscribers; time spent on site; the number of pages visited; and frequency of visits and conversations. While some social media sites may not provide all of the data listed, all offer some analytics.

- Sentiment: Tracking what customers are saying about a brand online is important in identifying opportunities to maintain or improve their view of the brand. Sentiment can be measured by a third-party automated platform or it can be measured manually with the use of Google Alerts, Technorati, Twitter Search and other free online tools. Analyzing the sentiment and topics discussed will help manage brand reputation, identify influencers, and identify what products, services, and processes may need to be reviewed and improved.

- Brand Metrics: Traditional brand metrics, such as brand likeability, brand awareness, brand recall and purchase intent, are directly affected by the word of mouth and viral quality of social media. This is also directly correlated with measures of sentiment, (positive, neutral or negative), regarding the brand and are critical in mapping out a strategy for achieving financial objectives.

<u>Outcomes</u>

- Retention: With the launch of social media efforts, a company should also track customer retention rates. A measureable increase would indicate a successful social media program. If retention shows no uptick, it warrants a reevaluation of the social media strategy. An example of this is the number of 'fans' registered on a platform such as Facebook. An increase in 'fans' could be an immediate indicator of the effectiveness of a social media program. Conversely, a decline in the number of 'fans' or followers signals a need to reevaluate and adjust the current strategy.

- Customers: By tracking the number of total customers and identifying new clients who are in households or companies with existing customers, one can infer the value of word-of-mouth and viral marketing in cross-selling.

- Satisfaction Scores: Select social media channels, such as Facebook and Twitter, have become another barometer of customer satisfaction. Facebook's "Like" option, for example, is an easy, instantaneous way for users to signal satisfaction with a company's information, product or service. Other social media platforms offer a similar option. Unhappy users can use the same media to express dissatisfaction; and there are countless examples of consumers' use of Twitter to air their complaints with their circle of followers. Such speedy indicators of consumer attitudes permit companies to gauge the success of particular initiatives and to make adjustments quickly in response to public sentiment.

Depending on your company's size and clients' acceptance of social media, it can require less or more amount time to recognize success. In addition, providing management with measurable metrics will help increase overall understanding of how success in this space can affect the bottom line and company's direction.

References

"Seven Guidelines for Achieving ROI from Social Media."
http://www.emarketer.com/Reports/All/Emarketer_2000659.aspx

"Social Media ROI: Customer Engagement, Brand Interactivity, and Revenue."
http://www.aberdeen.com/aberdeen-library/6398/RA-social-media-marketing.aspx

"4 Winning Strategies for Social Media Optimization." http://mashable.com/2010/10/22/social-media-optimization/

"8 Social Media Trends Impacting Businesses." http://www.socialmediaexaminer.com/8-social-media-trends-impacting-businesses/ (http://www.smartbrief.com/research/)

H. Lack of Centralized Governance

Description
Given the permanent, fast-moving and universal nature of social media, misuse of these tools, intentional or not, may result in reputational, financial or legal harm to a company. A clear and well-publicized governance structure for overseeing and coordinating social media activity that enables employees to closely coordinate their activities across businesses and have a clear understanding of chain of command and accountability will ensure consistent messaging and preserve data security.

The lack of governance could result in a range of issues, including:

- Physical Security:
  - Lost data
  - Compromised technology security

- Reputation and Brand:
  - Lack of corporate-wide policy, strategy and content standards
  - Inconsistent process for vetting/approving requests to use social media
  - Inconsistent messaging
  - Confusion about process and accountability both internally and externally
  - Inconsistent crisis planning and communications

- Legal/Compliance:
  - Regulatory violations
  - Civil suits over content

- Human Resources:
  - Violation of labor regulations/laws
  - Need for disciplinary action against employee abuse

Mitigation
As a company develops a social media program, it's essential that it organize a group of individuals to manage and implement policies, strategy and procedures and ensure that social media efforts mesh with the company's culture, brand, and legal or regulatory requirements.

Three elements of good social media governance include executive management and involvement, an organizational structure for managing social media, and a clear policy and set of procedures.

Many experts note that companies that are just beginning to use social media tend to use a highly centralized top-down approach to managing and guiding social media use. As an institution becomes more adept at and confident with social media, a more flexible "hub and spoke" structure emerges that allows key social media users in business groups to use the tools as deemed appropriate so long as the use complies with company policy and procedure.

Therefore there isn't a one-size-fits-all model for managing social media and often the structure will evolve as a company's social media strategy matures. Many companies relegate oversight and management of social media to its marketing department, while other organizations see it as an extension of corporate communications but many experts argue that best practices demand a cross-department oversight.

Generally, experts describe three roles as key to managing social media:

- Overall strategist(s) and leader,
- Moderators or managers liaising with different parts of the company and serving as resources, and
- Key social media manager within the business units deploying social media that provide on-the-ground support, oversight and liaison with the social media moderators and leadership of social media efforts.

Ultimately, the optimal governance requires full collaboration among the key users of these tools, such as PR/Media Relations, Marketing and Human Resources. Social media oversight is strongest in companies with cross-departmental participation to include Legal and Compliance, Technology Risk Management, and other departments identified within the institution. (See Appendix C.)

References
"How to Organize Your Company for Social Computing," Forrester Research recommendations on governance and ownership (fee-based report), http://www.forrester.com/rb/Research/organize_company_for_social_computing/q/id/47666/t/2

"Developing an Effective Governance Framework for Social Media," By Jess Wilkens, CRM AIIM International, http://www.slideshare.net/jessewilkins/20110323-info360-2011-social-media-governance

"How to Staff for Social Computing," Forrester Research: Who would oversee social media and what skills are needed (fee-based report), http://www.forrester.com/rb/Research/staff_for_social_computing/q/id/45127/t/2

"Companies Should Organize for Social Media in a 'Hub and Spoke' Model," Forrester Research: How should a company organize its or social media program? Which roles are needed? Which department is in charge? (fee-based report), http://www.web-strategist.com/blog/2009/06/25/report-companies-should-organize-for-social-media-in-hub-and-spoke/

I. Physical Security Risk

Description
Revealing too much in social media may pose a physical security threat. The National Center for Victims of Crime (NCVC) states "the attractions of social networking-access to an ever-widening

world of "friends"-can lead users to overlook the pitfalls of these sites. Young people, in particular, may tend to view such sites as "part of their own little world," not a public bulletin board with millions of other visitors. They may not recognize that posting personal information may lead to contacts from sexual predators, identity theft, fraud, or stalking--or that anyone could post a bogus profile to disparage, misrepresent, harass, threaten, or embarrass them."

Physical security threats are not limited to stalking. When senior executives use social media to advertise their physical location or travel agenda, additional personal risk may be created for these individuals. The real-time nature of the social networking sites creates a new risk to be considered. Anyone contemplating physical harm to a corporation's executive staff or board member would potentially have unprecedented access to information about an executive "Tweeter." This also applies to the physical safety of associates. For example, disgruntled borrowers may present physical risk to associates who have represented the company interests but also make their physical location known publicly.

As parents and practitioners of social media we are aware of the bullying aspect of the various channels in addition to the threat of identity theft. We are cautioned, and caution others, to not post information such as year of birth, social security number, or any other identifiable information. What is not communicated enough is the threat of stalkers utilizing social media to exploit their victims. Stalking is defined by the NCVC as "*a course of conduct directed at a specific person that would cause a reasonable person to feel fear.*"

With the advent of GPS technology and Foursquare, we are increasingly making it easy for someone to find our exact location. We post what we're doing, where we are, and typically who we're with which results in providing a treasure map for the stalker to his victim.

Additionally, geo-tagging capabilities for photos, now offered by sites such as Flicker, create a unique opportunity for interested parties to obtain information that may be otherwise considered proprietary information. For example, if an astute analyst follows an executive online and sees that he posts information from a site where the business may be considering a merger, the analyst may effectively have insider information without ever seeing an official communication. In international situations, kidnapping has presented a risk to some businesses.

Stalking statistics from 2009:

- 1 in 4 victims report being stalked through the use of some form of technology (such as email or instant messaging).
- 10% of victims report being monitored with global positioning systems (GPS), and 8% report being monitored through video or digital cameras, or listening devices.

Mitigation

NCVC has a wealth of information to help users of social media avoid becoming victims of stalking, which includes the following tips for social media use.

- Limit the information you share on social media sites. Don't provide information that makes it easy for a stalker to identify your current location, favorite activities, school, home, or even your favorite coffee shop.
- Keep your personal information private. Don't post your full name, social security number, address, phone number, or birth year — and don't post other people's information, either.

- Know your "friends." Don't "friend" someone you don't personally know. Stalkers are masters at creating fake personas in order to connect with unknowing victims.
- Be alert and be wary. When all else fails, remove your social media accounts.

J. Social Media Content Is Forever

Description

It has been estimated that of the 1.2 zettabytes of information in the digital universe, 95% is unstructured, and 70% is user-generated content. For any company of size, the odds are good that there is a large amount of information, positive and negative, about that company posted outside "official" communication or marketing channels. Large companies have a broad exposure to negative content posted on the Internet. This content can take many forms:

- Complaints about product or service
- Inflammatory content with the intent to disparage the reputation of the company or boycott products
- Company employees (and those posing as employees) posting accounts of negative experiences, internal practices or policies
- Employees leaking sensitive information, accidentally or purposefully.

Mitigation

Companies may struggle with determining whether they should make efforts to mitigate these events when they occur, and if so, how. Over just the past year a number of companies have been embarrassed by negative social content via multiple social tools:

Kenneth Cole: Twitter, http://www.mediabistro.com/prnewser/kenneth-coles-twitter-fail_b14367#)

KFC: YouTube, http://mashable.com/2010/01/10/kfc-ad-racist-youtube/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Mashable+%28Mashable%29#

Fonterra Dairy: Facebook, http://www.3news.co.nz/Fonterra-commits-Facebook-suicide/tabid/421/articleID/183903/Default.aspx

'Cook Source' Blog: Blog, http://www.digitaljournal.com/article/300451

Deciding whether or how to control negative social media events should take into consideration whether the nature of the event is:

- A non-sanctioned employee-initiated event
  - While using company property/networks
  - While on their own time and equipment, off company premises.
- A sanctioned company-initiated event
  - A marketing strategy gone awry (unintended consequence to a controlled campaign)
  - An employee acting on behalf of the company exhibiting poor judgment, such as treating a customer poorly on a public site.

In the first case, the company does not have access control to the platform or content. Accounts or passwords are maintained by the employee or other parties. The company must carefully weigh the benefits of directly contacting the hosting provider to request content removal. Many companies will decide that the risk of actively seeking to edit or remove social media is not worth the benefit. This draws even more attention to the content, and other negative backlash can result such as news of the company acting in a way that stifles freedom of expression or legitimate criticism.

In the second case, the company has control over the platform or account and can actively manage the offending content. In these cases, the company must weigh the benefits of removing offending or controversial content versus leaving it exposed but putting mitigating controls around it such as:

- Language that explains the situation and softens the impact
- Editing the content (redaction or correction)
- "Locking" the content to prevent further discussion
- Outright removal of the content.

In many cases, removal of the content does not also remove the context, and other non-controlled parties may have quoted it, copied it, or cross-posted it to other channels outside the control of the company.

Some platforms have methods for companies or individuals to "flag" inappropriate or incorrect content. These are usually human-moderated and sometimes only lock content from being edited or responded to but leave the original content up until a review is conducted, which can take some time and increases the risk that it will be copied.

Some online platforms allow companies to petition for content removal (e.g. YouTube). This is usually only allowed in cases of copyright or trademark infringement. If the offending content uses copyright material or company brand trademarks, it may be possible to request content removal on those grounds.

Sometimes a company will decide it is in its best interest to remove negative online content. The difficulty level varies according to the length of time the content has been in the wild, and the platform that is hosting it. See http://onlinereputationedge.com for a discussion of common types of online social media sites and the relative difficulty of controlling media posted to them.

Another strategy toward controlling negative online content is to not remove it but make it irrelevant. By careful use of online search engine terms, advertisement campaigns, and website creation, more positive entries can appear at the top of search results while negative results fall down or off the first few pages of search results. Although this does not actively remove content, it tends to push its importance down somewhat and people actively searching for information on a company will be less likely to be presented with negative online information about the company. Many marketing companies and online reputation companies have search engine optimization as a key service offering.

Additionally, there are companies such as Reputation Defender and iCrossing that are developing services that claim to act upon negative social media events on behalf of the company. Other brand protection and reputation companies such as Mark Monitor or Nielson Media Buzz have services that monitor brand reputation but do not yet have active mitigation services. Some companies must finally resort to legal action to control negative media events. These are typically events that have a significant risk to customers' privacy and security.

References
National Law Review Blog Feb 1, 2011, "Social Media: More Reasons to Pay Close Attention to What Your Employees Say and What Your Company Does About It,"
http://www.natlawreview.com/article/social-media-more-reasons-to-pay-close-attention-to-what-your-employees-say-and-what-your-co

Collective Intellect, "We have the Data – Now What??!! A few examples of Social Media Analytics,"
http://www.collectiveintellect.com/blog/we-have-the-data-now-what-a-few-examples-of-social-media-analytics

K. Lack of Associate Productivity

Description
The use of social media can be a contributing factor to lost productivity in the work place. According to a survey conducted in the summer of 2010 by People-OnTheGo, people spend more than 4.5 hours a day on email and social media combined. They admitted to spending one hour per day at work handling social media, including LinkedIn, Facebook and Twitter. Generation Y (those born after 1980) spend 1.8 hours per day on social media, and only 6.8% of that time had anything to do with work.

Lost productivity is not a new issue; social media is just a new contributing factor. Companies had similar concerns when they provided access to other technologies or opportunities, such as telephones, Internet/email, working from home, etc. Unproductive people will always find ways to be unproductive.

Mitigation
Lack of productivity due to the use of social media, like other factors that impact productivity (e.g., non-work related conversations with co-workers, personal phone calls, daydreaming, excessive breaks, etc.), is a people issue, not a technology issue.

Blocking social media sites is one way of reducing lost productivity due to use of social media. However, encouraging self-policing of social media use is a less offensive way of dealing with this issue. Additional solutions include:

- Create a social media policy which outlines expectations, acceptable behaviors and consequences.
- Provide proper supervision.
- Monitor use of social media sites.
- Look for ways to harness the use of social media in a positive and productive manner.

References
“Social Media in the Workplace: Can You Police Yourself?”
http://www.sandiegoreader.com/news/2010/dec/09/jobs-social-media-workplace/

Society for Human Resource Management, www.shrm.org

IV. REPUTATION

A. Reputational Threat

Description
Reputational threats are activities and/or information originating from employees or external sources that may damage the image and reputation of a company with all or some stakeholders, including actual and prospective clients and employees, regulators, lawmakers, members of the media, vendors and the general public.

Additional risk may arise from corporate failure to reply promptly to external requests for information from stakeholders named above.

Mitigation
A strong, cohesive and integrated governance structure for managing social media initiatives, as well as a cross-department escalation and crisis communication plan will provide an integrated approach to managing threats to corporate reputation.

<u>Training</u>
Training employees on social media use, risks, company policies and guidelines is the first line of defense for preventing inappropriate dissemination of content by employees and for sensitizing them to potential reputational risks from outside sources.

Training programs should cover:

- Who is permitted to use social media and the standard for gaining access
- What social media tools are permitted by the company and which are forbidden, how these tools work and their potential impact on company reputation
- All company guidelines for the frequency, style, tone and length of content
- Content that may be shared according to federal regulation and company policy
- All relevant corporate policies on code of conduct pertaining to external communications
- The review process for content before it is posted publicly
- The escalation process and when it is appropriate to activate it
- Consequences of inappropriate or unauthorized use of social media
- Personal use.

Employees should be trained upon hiring and this training should be repeated annually or semi-annually.

Once education and training is in place, a company should ensure employees understand what to do when a threat is detected. When a social media monitor detects confidential, negative or inaccurate information on a website, blog, microblog, video site or other online discussion forum they should immediately initiate a three-step escalation process. Timeliness is paramount so the escalation process must be set in motion in real-time.

Escalation Process

An institution should clearly identify reputational threats and the criteria for determining potential risk to a company's reputation. Below are different kinds of reputational threats that might arise:

- External transmission of confidential information about the company, its employees or clients (this may include instances of identity theft or hacking)
- Employee postings that contain company content (including advertising and marketing materials), or insensitive, offensive or inaccurate information
- Employee complaints and/or disparaging comments
- Client complaints about products or services
- Generally disparaging or inaccurate comments from members of the public
- Criticism from activist groups of company policies and/or practices
- Negative, inaccurate comments or news reports in print, broadcast or online
- Any of the above, compounded by company failure to respond in timely way.

Following is criteria that can be used to determine the scope and severity of the reputational threat:

- Credibility. Identify the site displaying the information and assess how "authoritative" or influential the source is with online users, especially members of the media.
- Audience. More than sheer numbers, if the audience is small but highly influential the threat could be much higher.
- Content. Assess the actual content for the degree of harm it poses to corporate image and reputation. This judgment is highly individual. What one company may classify as a high-level threat, another may see as low-level based on the attitudes of their stakeholders.

Once the threat has been assessed, employees should alert the appropriate individuals and/or departments within the company who can then take appropriate steps to respond. The relevant department(s), in concert with legal if necessary, would then decide whether to activate an escalation and crisis communication plan to address the risk. (Please refer to Responding to a Crisis Section.)

B. Lack of Monitoring

Description

To effectively use and manage social media, a company will need to closely monitor posts, tweets or comments regarding the firm, brand, executives and associates whether it be positive or negative. The use of social media may cause unintended consequences when not carefully guarded.

For example, an employee of a Securities Exchange Commission (SEC) regulated company posts an advertisement for the company's investment products on their personal Facebook page. The advertisements do not meet the Financial Industry Regulatory Authority (FINRA) requirements thus creating compliance risk for the company.

Conversely, social media may be used to promote the company and the brand. This may occur when a major financial institution monitors Twitter posts that cite the company's name. One tweet indicates a customer's extreme satisfaction with the Tweet servicing queue's ability to promptly resolve an account-related issue. The financial institution picks up the tweet and is able to retweet the information to help create a positive sentiment about the company.

Mitigation

Monitoring is a key risk mitigation technique for social media use. In order to have a successful monitoring plan, a corporation will need to create clear objectives for monitoring. Examples of objectives include monitoring for:

- Brand Comments and/or Perceptions
- Ad Campaign success
- Market Research
- Physical Security/ Labor Unrest
- Reputation Risk
- Compliance with Applicable Laws and Regulations.

Monitoring plans should include a clear response plan and escalation contacts for negative or harmful postings from both external and internal sources. Additionally some standards for immediate post/comment removal for inappropriate content should be in place. Training should be implemented for those doing the monitoring and all official interactive users.

The scope of monitoring should be defined as part of the monitoring plan. Since the Internet is virtually endless, it is imperative to prioritize your monitoring efforts.

The monitoring plan should include keywords that are relevant to your social networking efforts and marketing campaigns. At the least, you should consider tracking your company name, key executives, competitors, taglines and product names.

Various monitoring tools are available to support monitoring efforts. Tools should be selected that match your social media strategy. Some tools focus more on Twitter and Facebook, but may not support LinkedIn. Examples of social media monitoring tools include, but are not limited to:

Free Tools

- Google Alerts
- IceRocket
- Social Mention
- HootSuite
- Seesmic
- Tweetdeck
- Bit.ly

Fee-based Tools

- Radian 6
- Scoutlabs
- Sysomos
- Cyveillance
- SocialWare
- Brand Protect

This list does not constitute endorsement of any of the products listed above or within this paper.

C. Insufficient Employee Training

Description

Reputational and other forms of risk in use of social media can arise when employees, customers and other stakeholders are not made fully aware of a company's approved policy, procedures and strategy for proactive social media use.

Simply alerting employees that these documents exist and where they can be found on the company intranet is not enough to ensure that they understand their responsibility. Additionally, those employees authorized to communicate with the company's various audiences via social media must be fully fluent in use of these tools and be fully aware of their impact on the company's business goals.

Mitigation

Mitigation of such risks can include a corporate-wide PR campaign about social media use targeted to employees, training programs to familiarize select employees on social media tools and regular communications about social media use to increase awareness of risks and best practices.

Corporate Wide PR Campaign

A company should set about informing its employees and external audiences with a PR campaign about its social media program. The campaign internally will include messaging from key executives about the role social media will have in corporate communications, which would be followed with reminders for line managers to review corporate social media policy with staff and instruction on where to find additional information and resources.

Employee Training Program

Since employee involvement in social media will vary based on roles within the company, it might be more efficient to offer levels of training:

- High-level overview of social media in general that includes why and how the company did or plans to implement a social media program. The suitable audience for such an overview would be corporate officers and executives across the business in addition to employees that won't have tactical involvement with social media tools.

- More in-depth look at social media tools with specific demonstrations of how they work, including recommendations and a "how to" of the privacy settings for different platforms with a thorough review of company policy and procedures. This level of training would be appropriate for department heads of businesses that might be involved in social media as well as the managers of employees who are likely to participate in social media.

- Hands-on training in using the tools, best practices for privacy settings, crafting content that reflects the company's style, voice and corporate messaging, approval process, and retention and reporting procedures. This would be aimed at employees, including contract employees, who are involved with execution.

How such a program would be formatted and delivered will depend on a company's size, complexity and geographic reach.

It is also recommended to include training and best practices surrounding employees' personal use of social media from their private, not company, accounts, and the possible consequences of not doing so. For example, if an employee is made an administrator of the company Facebook page through a personal Facebook account and not attentive to page setting, the employee may end up in the embarrassing, and potentially brand-damaging, position of posting personal updates on the company's Facebook page.

To ensure that employees remain current on a company's social media program, such policies and procedures should be integrated into a company's annual review of corporate rules and code of conduct for employees.

Communications Plan

A company may also want to sensitize its clients and other external stakeholders of best practices and risks of using social media. For example, when users sign up or register to use corporate sponsored web pages or social media sites, they could be shown cautionary language against divulging personal information such as date of birth or social security or account numbers. Additionally, a company may offer tips to its clients on optimal privacy settings for the different social media platforms used. The detail in such a warning, however, should be highly individualized to that company's particular products and services, as well as its client base.

References

Harvard Business Review, Blogs: The Conversation. "Intel's Social Media Training,"
http://blogs.hbr.org/cs/2010/02/intels_social_media_employee_t.html

D. Negative Brand Impacts

Description

Missteps in use of social media by company employees, false or inaccurate information circulating through social media, or misuse of corporate trademarks, present potentially serious, long-lasting negative impact on a company's brand and reputation.

Company failure to respond quickly, decisively and in a positive way to negative commentary about its products, services or employees is another risk of negative brand impact.

Mitigation

To mitigate negative brand impact the following can be put into practice:

- A robust 24/7 monitoring system, also known as an Online Reputation Management platform (ORM), to listen for negative or defamatory content in real-time.
- As support to brand monitoring, a company must develop and implement a clear crisis communications plan that includes a step-by-step escalation process for directing negative commentary to the proper departments and individuals to handle.
- Additionally, timeline responses are important so client or report queries swift responses and escalation. A failure to respond in a timely way can reflect poorly on a company's commitment to client service, and hence the brand.
- However, each query must be handled on a per basis situation, thus a tiered response time outline is recommended. The outline should contain a minimum of three levels, high, medium and low, with definitions and examples of each to explicitly define each. A response time outline will allow employees to know expectations and respond within the correctly allotted time.
- Responses to comments and complaints must always be sincere and direct. Canned statements or stilted responses larded with legal jargon can easily backfire as shown in the Motrin case study below.
- Comprehensive, mandatory training is essential for staff charged with monitoring, assessing and escalating potential threats or client queries so that company response is prompt.

Case Study

In September of 2009, Motrin launched an ad campaign that focused on how wearing a baby sling can give backaches. However, it also gave an impression that baby slings were worn as a fashion statement.

After the ad was published, there was an online explosion of negative PR. One story in USA Today said it perfectly: "Offended moms get tweet revenge over Motrin ads." The controversy also was one of Advertising Age's Stories of the Year.

References

Motrin Moms- Case Study,
http://crisiscomm.wordpress.com/2009/01/28/motrin-moms-case-stud/

Anti-Phishing Working Group: a global industry and law association focused on eliminating fraud and identify theft through phishing, pharming and other means,
http://www.antiphishing.org/

E. Responding to a Crisis

Description

The viral nature of communications through social media means that a company's reputation can be instantly heightened or damaged with a hit of the <enter> key.

Today, a company's crisis communications plan must include both defensive use of social media (that is, a program to monitor online channels and identify and escalate threats) and proactive use of social media (to publicize company developments, engage with various stakeholders and to speedily address erroneous or malicious information that may be circulating online).

To detect and respond to negative content in a timely way, a company must continually monitor for threats to its reputation and image (see Monitoring Section) and have a plan for rapidly addressing those threats.

Mitigation

The most effective crisis planning and response involves an integrated effort among key parts of the company, including, but not limited to, Corporate Communications, Marketing, Legal, Information Technology and Human Resources.

An effective communications plan should include:

- Clear criteria for identifying risk that is likely to develop into a crisis
- An escalation process that details next steps in addressing the crisis
- Robust pre-crisis preparation, detailed responses for different kinds of crisis, and a process for evaluating the success of crisis response.

The plan outlined below is intended to supplement, not supplant, a company's existing crisis communications strategy to incorporate social media considerations. Each company will need to determine the best way of integrating these steps into their traditional crisis planning.

<u>Before a Crisis:</u>

- Regularly identify areas that are of higher risk to corporate image and reputation (i.e. executive compensation, loss of sensitive data, accounting errors, etc.) in context of current media coverage and discussion topics among influential bloggers and outlets.
- Make sure these issues are being monitored with your online reputation management platform.
- Develop a list of media outlets, bloggers and websites most likely to discuss or report on the key issues you consider most sensitive.
- Build and maintain relationships with key people in the media *before* a crisis arises and make sure that your media contact list is constantly updated.
- Develop guidelines to categorize different degrees of threat.
- Develop an escalation process/action plan [see below] appropriate for the level of seriousness of a threat. This plan should instruct media monitors to notify key communications executives and the wider communications team (including the social media users) about negative publicity and offer guidelines on responding. Additionally, this plan

should include a process for immediately shutting down certain functionality of social media access in the event of a security or information breach.

- Make sure the social media team is prepared to issue timely and accurate alerts if negative or erroneous information begins to circulate in traditional and new media.
- Work with your webmaster to create a link from the homepage of your website that links to a ghost web page for emergency information.
- When it makes sense, develop messaging in advance for "what if" scenarios.
- Designate key persons in various business lines who will manage the escalation process for addressing potential reputational risk.
- Identify who within corporate communications will handle social media issues and ensure this staff is aware of:
    - Who to contact internally when a crisis arises
    - Who will be a spokesperson(s) in various social media (think global not local) and ensure this staff has video training.
    - Process for developing messaging and getting approvals in timely way.
    - How to adapt messaging for social media and microblogging sites. For example, microcontent for Twitter or a video response.
    - How to work with appropriate social media point person(s) to distribute content.
- Coordinate with appropriate people in government relations, marketing and public relations (others as needed) to gauge public reaction to crisis communications efforts.
- Train staff to use necessary audio/video equipment to create and distribute content on website and/or YouTube.

Identify an Appropriate Communications Workflow

Before a crisis, determine the process to disseminate information to all appropriate departments. In addition to forwarding to Corporate Communications and Marketing staff, incoming messages posted on various sites or social media pages should be forwarded to the corresponding units below:

Job Queries: Forward to designated Human Resources (HR) social media user.

Product/Service Complaints and/or Angry Comments: Forward to the social media (SM) manager and corporate communications person serving the business involved. Those designees should pass along to appropriate marketing people for evaluation.

Generally these kinds of comments could be broken down into three or four levels of seriousness—it is up to each company to define the thresholds for their own crisis planning purposes.

- Low grade threat: Source is obscure; few followers; little traction or pick up; or the comments are disorganized, outlandish and not credible. [Example: "Martians are transmitting messages through the toaster oven I bought from company B."]
- Medium threat: Source is somewhat known but not widely followed; remarks are coherent and contain enough factual accuracy to warrant more immediate attention. Source has a critical mass of followers and some links to other credible sites. [Example: "My toaster oven made by company B gave off sparks and smoke, so I threw it away and everybody else who has one should do the same."]

- High threat: Source is established in the industry and has wide and/or influential following and links to key news outlets. Comments are credible, well-articulated. [Example: "There have been dozens of reports that toaster ovens made by company B overheat, sending off sparks and smoke. And the company hasn't issued any recalls."]

Praise, Compliments and/or Positive Notes: Forward as above.

Requests for Information: On products, services or a particular person, forward to social media manager of the relevant business, who will then route it to the right marketing person in the business and will be responsible for follow up. When the "case" is concluded, the date and person who handled it should be noted on the original request and forwarded to Corporate Communications and Marketing for archiving.

SPAM: File it away but keep count. If the same source is bombarding you with mail you should notify IT for potential action.

Reporter/Blogger/Media Outlet Requests: Forward immediately to Corporate Communications for follow up with reporter to connect him/her with the appropriate source. Time is of the essence for these kinds of queries.

<u>During a Crisis</u>

1. Those monitoring social media get the facts about the threat immediately and direct an alert to the person assigned to manage escalation in the business or division most immediately affected.

   Those facts include:

   - What happened (if this involves a breach of information or technology security)?
     - Who will be at risk? Employees? Company? Clients?
   - Where does this risk originate?
     - Should social media access be shut down pending investigation?
   - What was content of the commentary (if this involves externally generated information about the company)?
     - Is it opinion and hyperbole, or untrue or unfair charges?
   - What is public/stakeholder reaction to the charges? And, its potential to damage based on:
     - How "authoritative" the source is (Technorati and other tools are available to assist in determining this.)
     - The number of readers or followers that source has.
     - The "seriousness" of the information being circulated. For example, claims of corporate fraud would be far more serious than gossip about the cost of a CEO's birthday party.

2. Ask internal partners (legal, compliance, for example) and compare the facts with what is reported. Based on fact-finding you should determine:

   A. The appropriate response:
      - Refrain from responding but continue to monitor the outlet.
      - In the case of inaccurate information about the company, notify the source of the information and ask for a correction with facts countering the false claims.

- In case of private, offensive or inaccurate information improperly transmitted from within the company:
  - Immediately seek to withdraw the information from public view, if possible.
  - As appropriate or necessary, and in accordance with company crisis communications protocols, draft an explanation (or apology) acknowledging the problem and post on corporate website.
  - Immediately ask human resources, compliance and legal to determine if the problem was caused by an employee who had failed to follow policy for safeguarding confidential data.
  - Alert technology departments to determine if corporate IT security has been breached.

B. The message to convey to specific audiences
C. The channels to use for distributing the message
D. The appropriate spokesperson to deliver the message
E. How often you need to refresh information
F. Tactics to defuse negative publicity and possibly reframe it.

3. Continuously monitor social media through Online Reputation Management (ORM) and other tools (Radian6, PR Newswire) to gauge public reaction.
4. Record log of crisis activities and all data from monitoring for debriefing and reporting to Executive Committee.

<u>After a Crisis:</u>

- Summarize nature of the crisis
- Record what was done and how
- Use monitoring data, assess immediate and long-term effect on corporate image and reputation
- Confer with marketing for client reactions and include in summary
- Develop an after-crisis communication plan if appropriate
- Identify parts of execution for improvement and amend plan if needed.

A sample boilerplate internal/external statement in the event of an online problem:

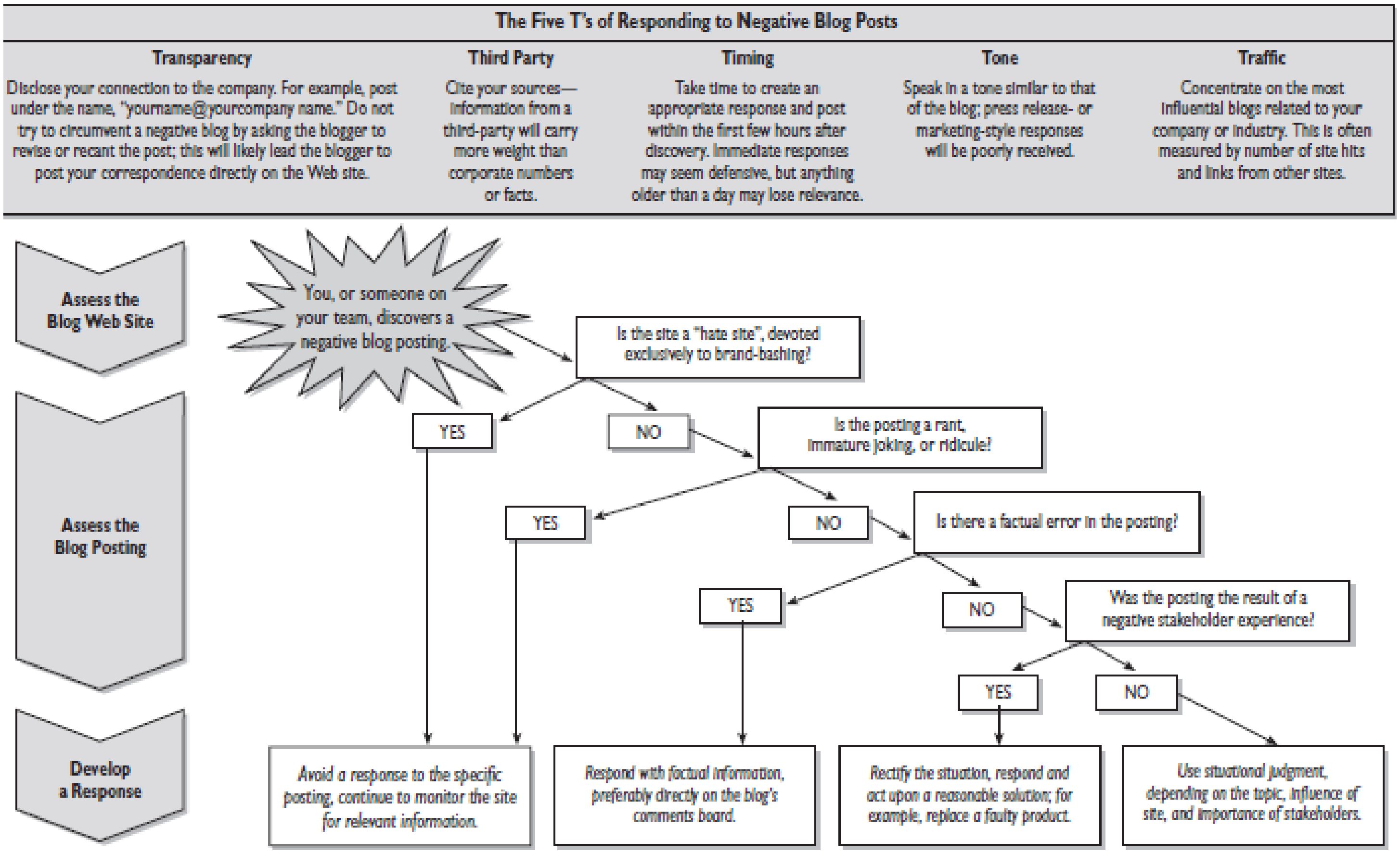
[Company] has been affected by a sustained and coordinated attack on our computer systems by external parties. Certain systems have been affected and we are working hard to establish the exact nature of the attack and are in the process of restoring the [site/system/operation]. A full investigation of the incident has begun.

References
ORM: Acronym for Online Reputation Management, a monitoring tool that scans the web for tweets, blog postings, forum comments, video and other digital media for content containing key words selected by the ORM user. Typically and ORM includes other capabilities including analytic tools for gauging tone of the comment, ranking the authority or importance of the source, and the number of followers or readers of a particular posting. ORMs also usually include a reporting function that allows a user to aggregate, organize and share the information for reporting purposes.

The Escalation diagram shows a process for addressing reputational threats from blog postings, but can be applied in a variety of online content presenting some kind of threat.

DECISION TREE

Responding to Blog Coverage: Guidelines to Help Shape Your Approach



The Five T's of Responding to Negative Blog Posts

Transparency	Third Party	Timing	Tone	Traffic
Disclose your connection to the company. For example, post under the name, "yourname@yourcompany name." Do not try to circumvent a negative blog by asking the blogger to revise or recant the post; this will likely lead the blogger to post your correspondence directly on the Web site.	Cite your sources—information from a third-party will carry more weight than corporate numbers or facts.	Take time to create an appropriate response and post within the first few hours after discovery. Immediate responses may seem defensive, but anything older than a day may lose relevance.	Speak in a tone similar to that of the blog; press release- or marketing-style responses will be poorly received.	Concentrate on the most influential blogs related to your company or industry. This is often measured by number of site hits and links from other sites.

Assess the Blog Web Site
Assess the Blog Posting
Develop a Response
You, or someone on your team, discovers a negative blog posting.
Is the site a "hate site", devoted exclusively to brand-bashing?
YES
NO
Is the posting a rant, immature joking, or ridicule?
YES
NO
Is there a factual error in the posting?
YES
NO
Was the posting the result of a negative stakeholder experience?
YES
NO
Avoid a response to the specific posting, continue to monitor the site for relevant information.
Respond with factual information, preferably directly on the blog's comments board.
Rectify the situation, respond and act upon a reasonable solution; for example, replace a faulty product.
Use situational judgment, depending on the topic, influence of site, and importance of stakeholders.

Source: Corporate Executive Board's Communications Executive Council

APPENDIX A - GLOSSARY

Account takeover identity theft occurs when a fraudster uses the victim's personal information to gain access to the victim's existing accounts.

Advanced Research Projects Agency Network (ARPANET) was the world's first operational packet switching network and the core network of a set that came to compose the global Internet.

Blog is a blend of the term *web log* and is a type of website or part of a website. Blogs are usually maintained by an individual with regular entries of commentary, descriptions of events, or other material such as graphics or video.

Blogger is a person who writes and posts to a blog.

Facebook is a social networking site founded by Harvard classmates in 2004. Most notably known for connecting with others as "friends."

ITAC, the Identity Theft Assistance Center, is a nonprofit coalition of financial services companies that was founded in 2004 by The Financial Services Roundtable and its technology affiliate, BITS, to protect financial institutions' customers from identity theft.

Microblog is similar to blog but the content is smaller in size and communication. Twitter is a microblogging tool.

MySpace is a social networking site started in August 2003 by eUniverse employees. MySpace was at its most popular in 2006 and until 2008 when it began to decline with the rise of Facebook.

Pharming is a technique of redirecting a user's or users' traffic to a fraudulent web site using DNS or a local host file. The attack is designed to capture credentials so that they can be used on the legitimate sites. Since the link comes from a trusted contact or from a social media presence thought to be trusted the user is less likely to scrutinize the page or SSL certificate error. This is a difficult attack to defend against because the users' desktops or their ISP's DNS servers and antivirus software will not detect it. [See Phishing]

Phishing or SmiSHing are techniques for fraudulently obtaining private information. Typically, the phisher sends an e-mail that appears to come from a legitimate business such as bank or a credit card company requesting "verification" of information and warning of negative consequences such as account closure if the information is not provided. The e-mail usually contains a link to a fraudulent web page with the company logos and content that looks like the legitimate site. This site would present a form requesting everything from a home address to a social security number or a password. SMiSHing uses this same mechanism, but instead of using email it uses a social media channels to engage the intended targets. Financial institutions should actively search for unauthorized or fraudulent social media identities and sites to mitigate some of the risk to their client base. [See Pharming]

Pretexting is the act of creating and using an invented scenario to engage a targeted victim in a manner that increases the chance that the victim will divulge information or perform actions that would be unlikely in ordinary circumstances. Pretexting most often involves prior research on the targeted victim and the use of prior information for impersonation (e.g., date of birth, social security number, last bill amount) to establish legitimacy in the mind of the target. Pretexting can also be used to impersonate co-workers, police, bank, tax authorities, insurance investigators or any other individual who could represent the authority or a legitimate business in the mind of the targeted victim.

<u>Retweet</u> is to repost a tweet from another user.

<u>Social Engineering</u> is the act of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical cracking techniques. The term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victim.

<u>Social Media</u> is a term used to define the relatively recent phenomenon of mass personal communication that is generally intended for public consumption often in an interactive and conversational style.

<u>Trojan horse</u> is software that appears to perform a desirable function for the user prior to install but then steals the information or harms the computer. A common Trojan horse is a program that claims to rid a computer of viruses but instead introduces viruses.

<u>True name identity theft</u> occurs when the fraudster uses the victim's personal information to open new accounts under the victim's name.

<u>Tweeter</u> is an account holder on Twitter who posts and reads Tweets. Also know as Twitters.

<u>Twitter</u> is a website owned and operated by Twitter Inc. which offers a social networking and microblogging service, enabling its users to send and read messages called *tweets*. Tweets are text-based posts composed of up to 140 characters displayed on the user's profile page. Tweets are publicly visible by default; however, senders can restrict message delivery to just their followers. Users may subscribe to other users' tweets – this is known as *following* and subscribers are known as *followers* or *tweeps* (Twitter + peeps).

<u>Virus</u>, or a computer virus is a computer program that can copy itself and infect a computer and it often referred to as types of malware, such as adware and spyware, programs that have reproductive abilities.

<u>Vishing or Phone phishing</u> is a technique using a rogue Interactive Voice Response (IVR) system to recreate a legitimate-sounding copy of a bank or other institution's IVR system. The victim is prompted (typically via a phishing email) to call in to the "bank" via a toll free number provided in order to "verify" information. A typical system will reject log-ins continually, ensuring the victim enters PINs or passwords multiple times, often disclosing several different passwords. More advanced systems transfer the victim to the attacker posing as a customer service agent for further questioning.

Web 2.0 refers to web applications used for interactive participation such as social networks, blogs, forums, etc.

Wiki is a website that allows the creation and editing of any number of interlinked web pages via a web browser.

Worm, or a computer worm is a self-replicating malware program that uses a computer network to send copies of itself to other computers in the network, potentially without any user intervention.

YouTube is a video-sharing website on which users can upload, share, and view videos, created by three former PayPal employees in February 2005.

APPENDIX B – BUILDING AN INTERNAL SOCIAL MEDIA TEAM: SUGGESTED MEMBERS

Subject Matter Experts	Tasks / Responsibilities
eBusiness/eCommerce/eMarketing	Develop strategy for use of Social Media
Legal	Research applicable domestic and international laws and regulations; develop disclaimers for associates to use for personal use; develop disclaimers for corporate use
Corporate Records	Define corporate record retention requirements; work with Technology to ensure an adequate archival solution is in place
Human Resources – Corporate	Implementing Policy; handle disciplinary actions for policy violations
Human Resources – Recruiters	Use as means to recruit new employees or to conduct background checks
Risk Management	Code of conduct impacts / assessments; establish if risk assessments are required
Corporate Communications	Communicating policy internally
Marketing/External Communications	Developing plans to communicate use of social media to customers, employees, potential employees, others; implement strategy for lines of business; advertising and publicity; monitor effectiveness
Community Manager	Moderate and monitor discussions; filter and/or direct content to other subject matter experts
Telephone Service Center	Use as means to communicate with customers
Collections	Use as means to communicate with customers regarding debts
Consumer	Use as means to communicate with customers (examples: retail banking and lending, personal lines' applications, policyholders' questions, retail investing); product marketing and delivery
Commercial	Use as means to communicate with customers (examples: commercial lending, commercial and industrial insurance, workers' compensation); product marketing and delivery
Claims Processing	Use as means to communicate with customers (examples: Reg

	E claims, insurance claims)
Business Continuity	Use as means to communicate with employees, vendors and customers
Institutional	Use as means to communicate with institutional customers and/or their customers (examples: Trust, 401K plans, broker / dealer, investment advisors); product marketing and delivery
Public Relations	Use as means to communicate media releases, economic/market commentaries, thought leadership, investor relations
Crisis Management	Use as means to communicate with media, employees, vendors, and customers during a crisis
Technology	Building infrastructure to support Information Security tools, content archives, and application development platforms
Information Security	Develop and/or provide input to risk assessments; managing internal access to social media sites; putting in tools to block inappropriate content from being posted
Intellectual Property	Defining intellectual property requirements
Privacy	Ensuring that privacy standards are met and policies are in place to prevent the release of non-public information on social media sites
Compliance	Ensure compliance with applicable laws and regulations; provide input to Corporate Records on retention requirements and to Legal on disclaimers
Field Office	Provide user experience and input
Quality/ Customer Satisfaction	Track customer experience and quality issues associated with this channel
Complaint Office	Monitor and/or respond to customer complaints made via this channel
Fraud	Monitor fraud associated with social media sites and develop strategies to address
Research and Advisory Firms; Consultants; Vendors	Research social media topics, tools, best practices
Internal Audit/ other Regulators	Review Risk Assessments

Project manager	Manage project tasks, schedule meetings, produce minutes
Insurance	Evaluate Cyber Liability Insurance needs with regard to social media exposures

Every institution uses different project methodologies. It is recommended that you have a Committee Chair who will develop the initial strategy statement(s) and convene the initial meeting of the Subject Matter Experts. Possible chairs might include: eBusiness/eCommerce, Marketing, Information Security, or Privacy Compliance. The meeting schedule, attendees, and task list can then be developed. As every institution has different organizational structures, you will need to select Subject Matter Experts as appropriate for your structure and/or policies.

APPENDIX C – BANKING REGULATORY AND LEGAL OVERVIEW[1]

Source	Reference	High Level Applicability
FRB	Equal Credit Opportunity Act – Regulation B	12 CFR 202.4 Discrimination related to offers and extension of credit (disparate treatment, disparate impact) 12 CFR 202.12 Record retention
FRB	Truth In Savings -Regulation DD	12 CFR 230.8 Advertisement 12 CFR 230.9 Record retention
FRB	Truth In Lending - Regulation Z	12 CFR 226.16 Advertisement Open-End Credit 12 CFR 226.24 Advertisement Closed-End Credit 12 CFR 226.24 Record retention
FRB	UDAP – Reg AA	12 CFR 227 Unfair and deceptive practices. (note: Under Dodd-Frank this will be expanded to UDAAP – Unfair Deceptive and Abusive Practices)
FCRA	Section 114 FACT Act - Identity Theft - Red Flag Rules	OCC 12 CFR Part 41 Detect, Mitigate and Prevention of Identity Theft FRB 12 CFR Part 222 Detect, Mitigate and Prevention of Identity Theft
FDIC	12 CFR 328	Advertisement of FDIC Membership
FDIC	FIL-80-98	Non-deposit Investment Products & Record Keeping requirements
FFIEC	Guidance on Electronic Financial Services & Consumer Compliance	Interagency guidance pertaining to federal consumer protection laws and regulations and their application to electronic financial service operations. (note: This document pre-dates the modification of several consumer regulations to incorporate eSign Act compliance.)
HUD	Fair Housing Act - 42 U.S.C. 3601	Equal Housing Logo & advertisement

[1] At this time, the banking agencies have not issued targeted guidance on the subject of Social Media, and none of the banking regulations have been modified to address social media considerations. Without targeted social media guidance or explicitly communicated exclusions from the agencies, financial institutions should consider that any regulation which applies to existing banking products, services and channels would also apply in the social media environment. The references cited in this appendix are provided only as a frame of reference and are not intended to be an exhaustive list. Since the applicability of laws and regulations is driven by how the financial institution chooses to use social media, the FI should perform an analysis of regulatory applicability based on the products or services within scope of the social media initiative.

	E-SIGN Act 15 USC 7001	Capture and retention of electronic consent
GLBA	Gramm-Leach-Bliley Act	Privacy and Safeguarding customer information, Information Sharing (third parties & affiliates), disclosure
FRCP	Federal Rules of Civil Procedures (Rules 16, 26, 33, 34, 37 and 45)	Records Management & Retention
FFIEC	IT Examination Handbook on Information Security	Information Security, Legal, Regulatory and Reputation Risk
OCC	Bulletin 2001-47	Vendor due diligence, Legal, Regulatory & Reputation Risk
OCC	Bulletin 2008-16	Web Application Security, vendor due diligence

APPENDIX D – OTHER APPLICABLE LAWS AND REGULATIONS

PCI Security Standards Council	PCI DSS	Disclosure of credit card number and retention of CVV
HHS	HiTech Act / HIPAA	Disclosure of personal medical information

APPENDIX E – SOCIAL MEDIA RISK MATRIX

Compliance

Risk Type	Primary Impacted Areas								Potential Applicability		
	Brand/ Marketing	HR	Legal	Risk Management	Public Relations	Internal Audit	Compliance	Information Security	Personal Use	Official Use – Internal	Official Use – External
Foreign and Domestic Privacy Laws		✓	✓	✓	✓		✓		✓		✓
Managing Compliance with other Company Policies		✓	✓	✓	✓		✓		✓		✓
Information Retention Management		✓	✓		✓	✓	✓				✓
Endorsement Guidelines (FTC)							✓				✓
Labor Relations					✓		✓				✓
Payment Card Industry			✓	✓			✓				✓
Marketing Laws and Regulations	✓		✓		✓		✓				✓
FINRA Requirements							✓		✓		✓

Legal											
Risk Type	**Primary Impacted Areas**								**Potential Applicability**		
	Brand/ Marketing	HR	Legal	Risk Management	Public Relations	Internal Audit	Compliance	Information Security	Personal Use	Official Use – Internal	Official Use – External
Lack of Separation of Personal and Professional Communication		✓	✓	✓						✓	✓
Civil Litigation		✓	✓	✓	✓	✓			✓		✓
eDiscovery			✓		✓	✓	✓				✓

Operational											
Risk Type	**Primary Impacted Areas**								**Potential Applicability**		
	Brand/ Marketing	HR	Legal	Risk Management	Public Relations	Internal Audit	Compliance	Information Security	Personal Use	Official Use – Internal	Official Use – External
Identity Theft		✓		✓	✓		✓	✓	✓		✓
Spreading Malware								✓			✓
Social Engineering		✓						✓			✓
Disclosure of Intellectual Property or other Sensitive Information	✓	✓	✓	✓	✓		✓	✓	✓		✓
Products Lack Maturity				✓	✓		✓	✓			✓
Managing Access		✓				✓		✓			✓
Measuring Success	✓										✓
Lack of Centralized Governance	✓					✓			✓		✓
Physical Security Risk			✓		✓			✓			✓
Social Media Content is Forever	✓		✓				✓				✓
Lack of Associate Productivity		✓							✓		

Reputation											
Risk Type	**Primary Impacted Areas**								**Potential Applicability**		
	Brand/ Marketing	HR	Legal	Risk Management	Public Relations	Internal Audit	Compliance	Information Security	Personal Use	Official Use – Internal	Official Use – External
Lack of Monitoring					✓		✓	✓			✓
Reputational Threat					✓						✓
Responding to a Crisis		✓	✓	✓	✓		✓				✓
Insufficient Employee Training		✓								✓	
Negative Brand Impacts				✓	✓						✓

ACKNOWLEDGMENTS

We would like to thank the following individuals for their contributions to this document:

Heather Ausmus, Alliant Credit Union
Lisa Matthews, Bank of America Corporation
Antonia Swann, BB&T
Susan Rivers, BNY Mellon Corporation
Amanda Barth, Capital One Financial Corporation
Cheryl Muzia, Comerica Incorporated
Alexander Popowycz, Fidelity Investments
Marge Fiedler, Harris Bankcorp, Inc.
Ellen Jackson, KeyCorp
Marc Loewenthal, LPL Financial
Robert Reh, Nassau Financial Federal Credit Union
Denise Watson, Raymond James Financial, Inc.
Michele Cantley, Regions Financial Corporation
Stephanie Becker, The Charles Schwab Corporation
Kaya Westling, Wells Fargo & Company
Sally Wiese, Wells Fargo & Company

BITS Staff Lead: Andrew Kennedy

About BITS
BITS addresses issues at the intersection of financial services, technology and public policy, where industry cooperation serves the public good, such as critical infrastructure protection, fraud prevention, and the safety of financial services. BITS is the technology policy division of The Financial Services Roundtable, which represents 100 of the largest integrated financial services companies providing banking, insurance, and investment products and services to the American consumer. For more information, go to http://www.bits.org/.