

TO THE NEW

The worst of all social media risks is thinking that it doesn't exist

SOCIAL RISK

social media

CAUTION CAUTION CAUTION CAUTION CAUTION CAUTION

Social Networking – Business, Compliance & Audit Implications 1

Agenda

- ➔ **What it is & How it is used**
- Survey Results**
- Various Risks / Issues**
- Audit & Control Implications**
- Risk Mitigation**
- Sample Audit Findings**

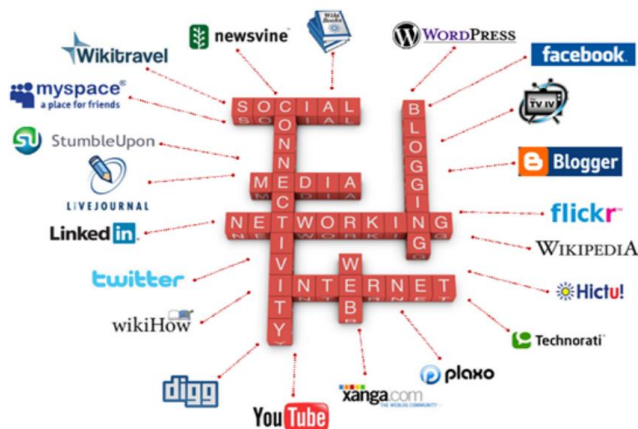
Social Networking – Business, Compliance & Audit Implications 2

Social Networking Defined

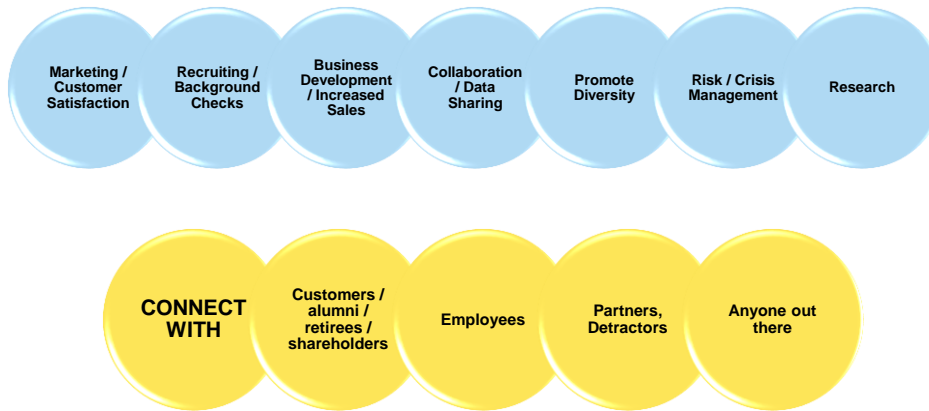
“A social network is a **social structure** made up of individuals (or organizations) called "nodes", which are tied (connected) by one or more specific types of **interdependency**, such as friendship, kinship, common interest, financial exchange, dislike, sexual relationships, or relationships of beliefs, knowledge or prestige.”



Social Networking Landscape



Uses of Social Networks



Uses of Social Networks



Benefits to Company

Increase employee productivity and operational efficiencies

Communications Platform

Foster creativity, innovation and collaboration

Brand Recognition

Enhance customer and partner relationships

Challenges to Company

Rapidly evolving ecosystem

Unclear and changing regulatory requirements

Lack of transparency on use

Difficulty of estimating risks

Unknown or many owners for SM risks

Is it Widespread?



Is Your Company Here?

Per minute, 4.17 million posts are liked in Facebook, 347,222 tweets are sent, 300 hours of video are uploaded on YouTube, 1.74 million photos are liked on [Instagram](#), and 9,722 images are pinned on [Pinterest](#).

Agenda

- What it is & How it is used
- Survey Results
- Various Risks / Issues
- Audit & Control Implications
- Risk Mitigation
- Sample Audit Findings

Clearswift Survey



Generation Web 2.0 Workers May Prefer Facebook Perks Over More Pay

The headline figure from Clearswift's resulting report, "Web 2.0 in the Workplace," is that over 79% of respondents said that the most important feature of a workplace for them, above job title and even pay, is to be trusted to **organize their own work schedule and have free access to the Net.**

Some 62% of workers thought it should be allowable to use social networking services from their desk for their own private purposes. Just 51% of management-level respondees had the same viewpoint.

Clearswift Survey

Generation Standby

57% of 25 to 34 year-olds already are social networking, shopping, and reading personal email at work.

21% said they'd turn down the offer of a job that was otherwise good, but forbade access to the Net and Facebook, Twitter and so on.

Increasingly connected to the world digitally - we're constantly awaiting the next digital hit, and even expect it to be a norm while working.

Social Business Benchmark 2014

Percent	Response
88%	The organization's social media presence is important to the bottom line to stay competitive
86%	Analyzing data helps the bottom line, BUT
41%	* Fully capitalize on the data captured by social media
60%	* Information is valuable but challenges remain to turn it into something actionable
30%	Social media strategy is very integrated / completely aligned across various departments in the company
64%	Aligning it in same fashion was difficult

Social Business Benchmark 2014

Percent	Response
	Social Media is valuable in the following ways:
84%	Enhancing relationships with existing customers
84%	Engaging with influencers
81%	Learning about the company's reputation
79%	Monitoring external communication
73%	Resolving customer complaints / questions
54%	Vetting potential employees

Social Business Benchmark 2014

Percent	Response
72%	Number of departments using it is growing
80%	Using it for analytics
78%	Using it to measure campaign results
79%	Use it to manage multiple accounts
79%	Maintaining security of SM accounts is critical
74%	Listening / monitoring conversation is important
74%	Have ability to execute campaigns across multiple accounts

Agenda

- What it is & How it is used
- Survey Results
- Various Risks / Issues
- Audit & Control Implications
- Risk Mitigation
- Sample Audit Findings

Threats / Risks

Threat

- **Exposure to customers and the enterprise through a fraudulent or hijacked corporate presence**

Risks

- Customer backlash/adverse legal actions
- Exposure of customer information
- Reputational damage
- Targeted phishing attacks on customers or employees

Mitigation / Control

- Develop brand protection guidelines and assign staff or hire a firm that can scan the Internet and search out misuse of the enterprise brand
- Give periodic informational updates to customers to maintain awareness of potential fraud

Threats / Risks

Threat

- **The move to a digital business model may increase customer service expectations**

Risks

- Customer dissatisfaction with the responsiveness received on social media sites, leading to potential reputational damage for the enterprise
- Customer retention issues

Mitigation / Control

- Ensure that staffing is adequate to handle the amount of traffic that could be created from a social media presence
- Create notices that provide clear windows for customer response
- Content to establish expectations

Threats / Risks

Threat

- Use of personal accounts to communicate work-related information

Risks

- Privacy violations
- Reputational damage
- Loss of competitive advantage
- Trade secret exposure
- Transmission of sensitive data

Mitigation / Control

- Work with the HR department to establish new policies or ensure that existing policies address employee posting of work-related information
- Work with the HR department to develop awareness training and campaigns that reinforce these policies

Risks



Risk: Strategy

Lack of Strategy

- “This looks cool. Somebody do something.”
- No plan, concepts, leadership
- Dive in, swim and hope you get there

Pseudo-Strategies

- Ignoring Social Media
- Dismiss Social Media as not worth the time
- No deliberation about the proper approach

Opportunity Risk

- Missing out on Social Networking may impact finances or reach the next generation of consumers, users, and stakeholders.
- Non-participation = non-involvement
- People will be talking even if the company doesn't lead the conversation

Risk: Strategy

A Good Strategy

Strategy, not just tactics

Alignment with business objectives

Set targets and measure performance

Long-term vs. short-term strategies

Incorporation of social media into all strategies

More Complete Strategy

Identification of target audience

Two-way communication model

Identification of social media channels

Retain control of content being posted

Resources properly allocated

Risk: Strategy

Focuses on strategy, not tactics

Has a value proposition

Addresses real customer needs

Implementation groundwork

Appropriately documented

Risk: Governance

No Group Responsible

Initiatives started in various places

No "champion" for overall initiatives

Poor communication, unclear authority, and mixed messages

Missed Risks & Rewards

Too much focus on risks

No understanding of rewards

Focus on controls versus opportunities

New opportunities missed

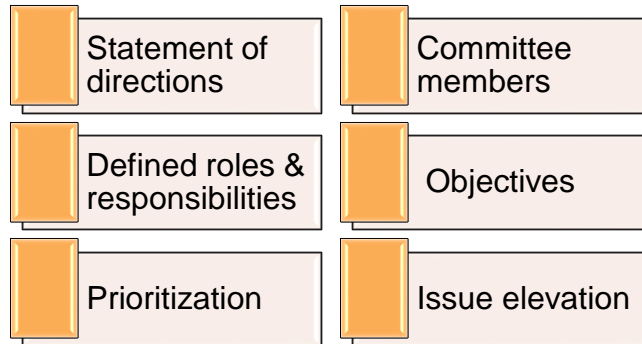
Wrong Group in Charge

There is no "wrong" business unit

Unit may be too focused on risk or technology issues

Examples include Risk, Compliance, IT, or Legal

Governance = Social Media Committee



Risk: Metrics

Metrics

- None
- Misaligned with goals
- Poor metrics

Poor Metric No alignment

- Website hits
- Blog comments
- Facebook friends
- Twitter followers

Good Metric Aligns with the organization's metrics

- Brand Recognition: Advocate Numbers and Frequency
- Sales & Marketing: Sales Generated
- Customer Service: Issue Resolution Rate
- Human Resources: Potential Candidate Engagement

7 deadly sins

1. PRIDE:

- Over-sharing company activities - excited about something the company is working on and must tell everyone about it.

2. ENVY:

- Mixing personal with professional. Uses a social network for both business and pleasure, most commonly on Facebook.

3. WRATH

- Engaging in SM rage
- Person just laid off fires back with a stream of vitriol can be irresistible

4. GREED

- It's about accumulating as many connections as possible.
- Quantity over quality: easy to link or "friend" a scam artist, terrorist or identity thief.

7 deadly sins

5. Sloth

- Sin of laziness, picking passwords for your social networks least likely to forget. Worst case: same password for LinkedIn and Facebook as for online bank account or work machine.

6. Gluttony

- Clicking everything. For some social networkers, clicking on such requests is as natural as breathing. The bad guys know this and will send links that appear to be from legitimate friends.

7. Lust

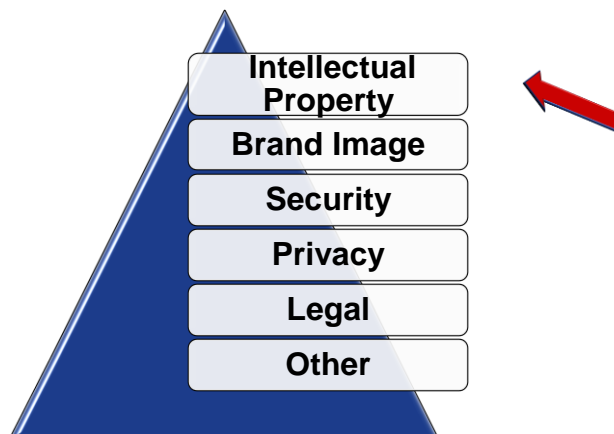
- Reckless social networking can literally put someone's life in danger. It could be a relative or co-worker. Or it could be yourself.

Risks Costs



Symantec: 2014

Various Issues



Intellectual Property Issues

Exposure of Confidential / Proprietary Files

Scribd, Box.net and Slideshare – uploading company files

YouTube – uploading videos

Some sites claim they own data posted on site

Copyright infringement - sites like Scribd have recently been sued for copyright infringement

IP Issues

Protecting the company's IP

Determining who owns what

Avoiding claims by third parties

Protecting your own IP

- **Online posting of confidential information**
 - Trade secrets lose protection once they no longer are secret
- **Misuse of company name, marks and logos**
 - Failure to police misuse of marks can lead to loss of rights
 - What are you allowing channel partners and others to do with your brand?

Who owns what

Are online identities property of employer or employee?

What about blogs, postings, etc.

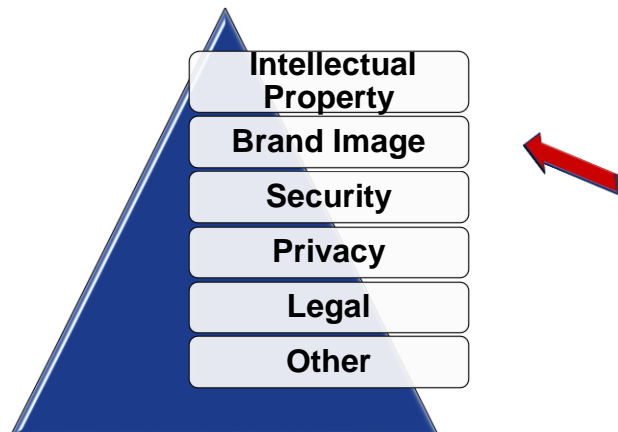
Particularly important when an employee departs

Can be addressed in policies or employment contracts

Third Party Claims

- Protect against employee infringement of third party IP
 - Posting text, images, or recordings (audio or video) may infringe IP rights of others
- Companies that allow posting of User Generated Content (UGC) not liable for defamatory, deceptive or otherwise harmful *third-party* content.
- *But* immunity may be lost if website agrees to remove content and fails to do so.

Various Issues



Brand Image

Misuse of logos

- Sites use corporate logo, gives users the perception of an officially corporate sponsored group
- Logos are of great value and companies go to great lengths to protect their brands

Improper blogging and inappropriate comments

Loss of competitive advantage and customer confidence

Defamation and Copyright Infringement

Dissemination of false or fraudulent information

Brand Image

Voice of the customer is amplified

Who is watching

Unofficial spokesperson(s)

Regulators

Crisis Management

What Would Help

Social Media Policy

- Internal
- External

Monitoring

3rd Party Oversight

Reputation DR

Brand Image

- **VW Emission scandal (9/15)**
- **Many people did not post negative comments about the company**
- **People seem to be outraged at the negative publicity**

Brand Image – Website Magazine

CEOs

Chief executive officers (CEOs) must be visionaries.

First spokesman to amplify the product message by maintaining a public profile on social platforms and a personal blog/website.

Charged with “shaping the market” as a thought leader. He/she must also become the face of the company on social media.

Only 32% have at least one profile on a social media page. The CEO of a product personal in nature to the consumer sb genuine and bold on social media and in real life.

Is acting as the chief spokesperson – the one who sets the tone for the entire brand.

Needs to be very careful - accountable for the company/shareholders in terms of whatever they say and do online and off.

Brand Image

HubSpot Blog

4 Ways Social Media Helped Gap's Logo Disaster

Inbound Internet Marketing Blog

SFO, Blogging, Social Media, Landing Pages, Lead Generation and Analytics

Posted by Billy Macdonald

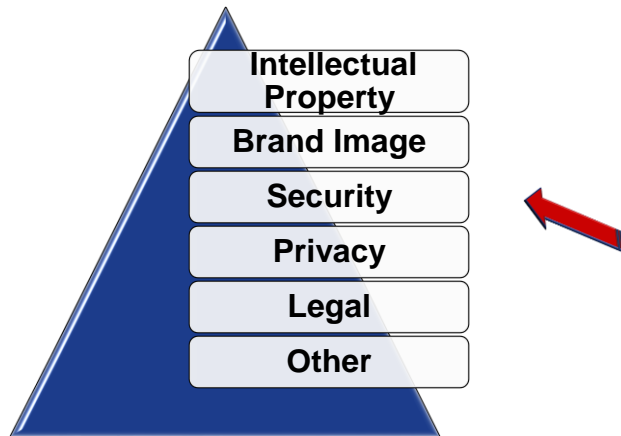
Wed, Oct 13, 2010 @ 06:00 PM

Lead Generation | Public Relations | Web Analytics | Web Design

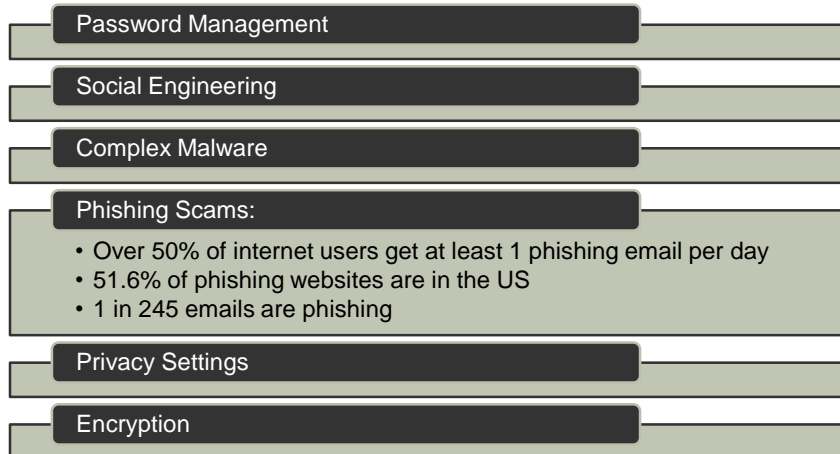
Last week Gap used Facebook to announce their plans for a new logo and was hit with mass amounts of negative feedback. Despite mainly getting discouraging comments and even a few websites designed to specifically make fun of the new logo, Gap may have actually **made out** in their decision to inform their social network first.

1. Trust Within Their Network
2. Saving Money on Rebranding Deployment
3. Generated Buzz
4. Understanding Where to Get Future Feedback

Various Issues



Security Issues



Security Issues

Spoofing of accounts

Same Passwords - not changed regularly or ever

Viruses and malware

Organized crime and targeted attacks

Employees as the weakest link

Physical security

Cyberstalking: Burglars using Facebook and Twitter to target homes whose owners are away

Security Issues

SPIM (SPAM over Instant Messaging)

Account Hijacking

Unauthorized Monitoring

Data Leakage / Loss Prevention (DLP)

High Cost of Governance

- Tools
- Monitoring of communications
- Performance impact to network
- Complexity of solutions

Security Issues

Security policies do not encompass these technologies and interactions

Trust but verify

57% of social networking users report being hit by spam via the services of social networking

Nothing to stop someone from using your screen name on other services

**Cisco Survey: 1 in 10 have IT directly involved.
Too many groups – who's in charge?**

Security Measures

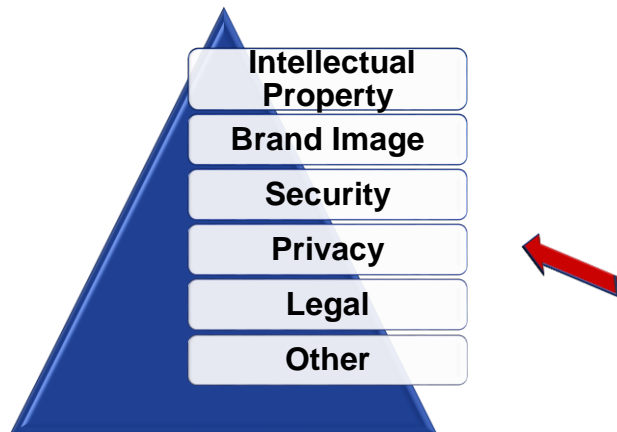
Login: Protect each of your accounts with a strong, unique password and do not share them. Some sites support stronger authentication, such as two-step verification. Do not use your social media account to log in to other sites.

Privacy Settings: review and test them regularly. Many apps and services let you tag your location to content that you post - regularly check these settings if you wish to keep your physical location private

Encryption: Social media sites use encryption (HTTPS) - sites (like Twitter and Google+) enable this by default. Others require it to be manually enabled. Check your social media account settings and enable HTTPS as the default connection whenever possible.

Malicious Links/Scams: Be cautious of suspicious links or potential scams. Just because a message is posted by a friend does not mean that message is really from them.

Various Issues



Privacy Issues

• Easy to provide too much information about you and company

• Personal information available to a wide audience

• No confirmation that people are who they say they are (trust & verify)

• Encryption of data storage and in use is questionable

• Protection may not be a high priority for the service provider

• Loss of Fourth Amendment protection

Privacy Issues

Social media sites have become the go-to places where employers, college admissions officers and divorce lawyers can perform background checks

Armed with the information, police caught fugitives, lawyers discredited witnesses and companies discovered perfect-on-paper applicants engaged in illegal or simply embarrassing behavior

Insurance companies will bring up anything — photos of you drinking to prove that you have bad character

Privacy Issues

Data leaks continue to embarrass firms who do not put data loss protection and encryption in place

More attacks against cloud-based systems as more end-users trust their personal information to the internet

More accusations of cyber warfare and industrial espionage –perpetrated by cybercriminals

Privacy Safeguards

Impacting Your Future

- Embarrassing or incriminating photos or posts, no matter how old, could prevent you from getting hired or promoted.
- Privacy options may not protect you, as these organizations can ask you to “Like” or join their pages or certain posts may be archived on multiple sites

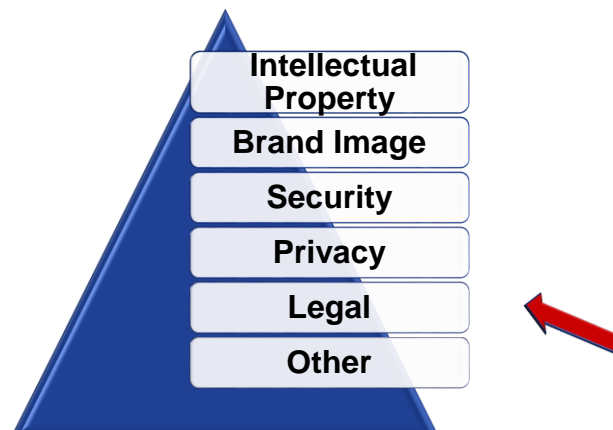
Attacks Against You

- Cyber attackers can analyze your posts and use them to gain access to your or your organization's information.
- These attacks can spill into the physical world: identifying where you work or live.

Accidentally Harming Your Employer

- Criminals or competitors can use any sensitive information you post about your organization against your employer, possibly causing reputational harm for your organization.

Various Issues



Legal Issues

Discrimination

Discriminatory comments about fellow employees, customers, or clients of the company expose both the employee and the employer to the risk of expensive discrimination claims.

Harassment

Employee may violate a fellow employee's dignity by creating an intimidating, humiliating, offensive, or degrading work environment through forum comments or blog postings.

Legal Issues

Disclosure of non-public information

Trade secrets, patentable information, and financial data undermines a company's competitive position and may endanger its ability to obtain a patent or maintain its stock price in the market.

Personal privacy

Employees who reveal sensitive personal information about their colleagues, such as e-mail addresses, may cause significant problems in the workplace.

Legal Issues

Breach

Forty-six states, the District of Columbia, Puerto Rico, and the Virgin Islands have legislation requiring notification of security breaches involving personal information.

In addition, Federal regulations, such as the Health Information Technology for Economic and Clinical Health, have breach notification clauses.

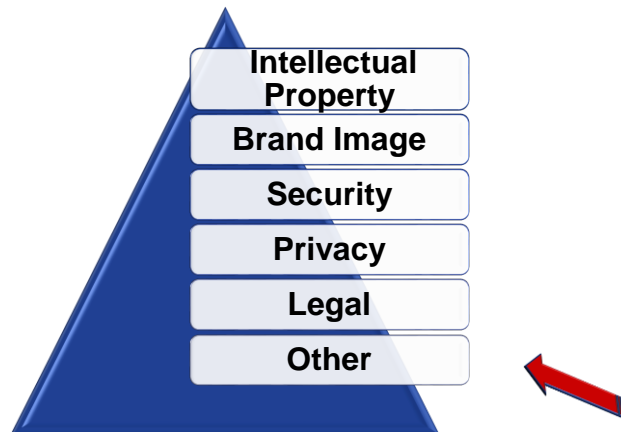
Legal Issues

E-Discovery

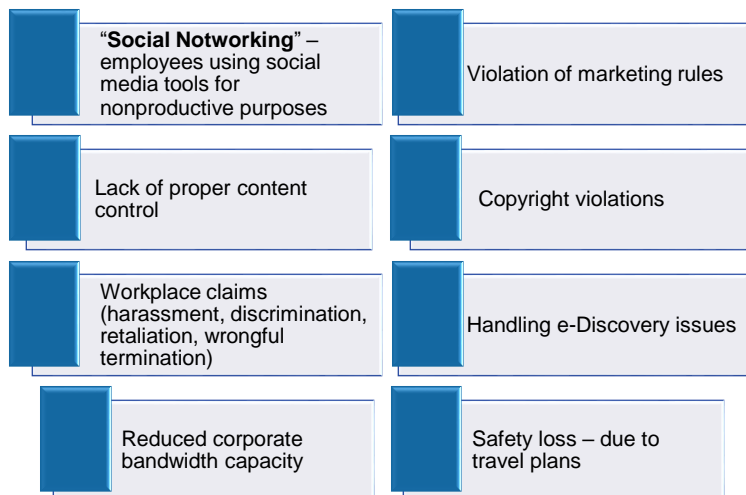
In a 2013 survey of in-house counsel, 20% indicated that they'd had to turn over content from employee social media profiles during internal investigations or during discovery in litigation.

Difficulty of preserving texts, call logs, and other Electronically Stored Information (ESI) on mobile devices for the typical 1-2 year legal hold period, and (for global companies) compliance with increasingly stringent EU data privacy laws when corporate ESI gets commingled with personal texts, chats, and other personal ESI.

Various Issues



Other Issues



Disgruntled employee posts false or insider information about the company which is then sued by shareholders

Other Issues

Human Error: mistakes are bound to happen. Employees may also be hacked because they trust fellow members and may be tricked by fraudsters.

Processes: Firms need to define and approve the right permissions, approvals, access, data classifications and collaboration processes before they get started.

Legal: adherence with privacy laws, to content ownership, to intellectual property infringement, to human resources

Data: meet the regulatory requirements of collecting, processing, handling and storing data. Global firms need to comply with local data protection regulations when employees are connecting with each other and sharing documents across borders.

Companies Should

Never Use
A Competitor's
Product Especially
When Posting On
Social Media

Know The Context
Of A Trending
Hashtag Before
Jumping In On The
Trend

Never Open Up
A Q&A Trend You
Aren't Prepared To
Handle

Be Sensitive With
Your Posts To Avoid
Negative Reactions
From Netizens

Be Reminded That
You Carry Your
Brand Even In Your
Personal Accounts

The Greatest Lessons From Epic Social Media Fails 2015
March 24, 2016 [Social Media Marketing](#), [Social Media](#)

Agenda

- What it is & How it is used
- Survey Results
- Various Issues
- Audit & Control Implications
- Risk Mitigation
- Sample Audit Findings

Corporate Executive Board

Audit Plan Hot Spots - #4

Companies are increasingly using social media channels to collaborate, communicate, and share information, both internally as well as with clients

However, most companies are doing so without proper governance and controls which gives rise to significant business, legal and regulatory risks

Corporate Executive Board

Audit Plan Additions

- **Social Media Policy Audit**—Review the existence and adherence to corporate policies on employees' personal and corporate social media usage.
- **Activity Monitoring Check**—Ensure that IT regularly monitors employees' usage of social networking channels, while on the corporate network, and takes appropriate action if employees are found violating usage guidelines.
- **Content Modification Review**—Review the policy and process by which IT removes or modifies certain comments and posts.
- **Archiving Process Audit**—Assess the effectiveness and adherence to policies in place that provide content archiving guidelines and timeframes, so that these official records are more than adequate to serve as evidence in case a legal issue arises.

Corporate Executive Board

RISKS INVOLVED

- **Brand or reputation damage**—Negative posts or comments about a company on any social networking Web site can seriously damage the company's brand image and goodwill in the market.
- **Regulatory and legal liability**—Disclosure of nonpublic, company-sensitive information could result in legal and regulatory repercussions.
- **Information loss**—Exchanging information through social media channels could lead to information loss as there aren't structured processes in place to secure and archive this information. This is specifically true for information exchanges through external social media.
- **Reduced corporate bandwidth capacity**—With companies increasingly allowing the use of Web 2.0 technologies, the number of employees logging onto these networks has increased, which is in turn putting pressure on the corporate bandwidth.

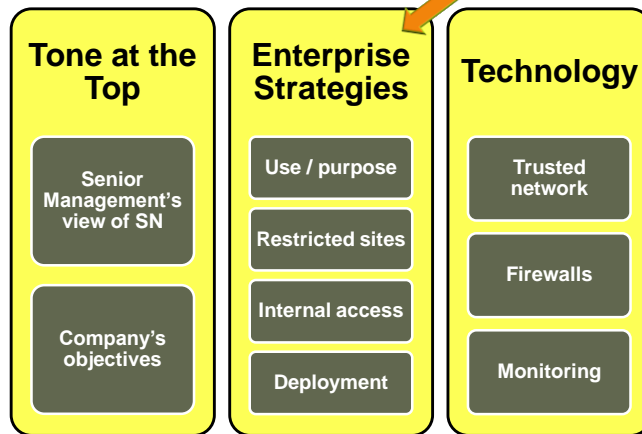
Audit and Control Implications



Controls Foundation



Controls Foundation



Enterprise Strategies

Enterprise Strategies

Alignment with business objectives

Long-term vs. short-term strategies

Incorporation of social media into all strategies

Identification of target audience, social media channels, resources properly allocated

Controls Foundation

Corporate Policies

Existence

Comprehensiveness

Frequency of review /
updating

Audit and Control Implications



SN Policy Structure

Purpose

- A growing number of employees participate in a variety of online communications, social media and networking activities such as personal blogs, Twitter, Facebook, LinkedIn, YouTube, etc.
- This policy is intended to provide direction to employees on appropriate conduct when engaging in Social Media Activity that identifies the employee's affiliation with the Company

Definitions

- Including but not limited to:
 - Postings on social networking sites (Facebook, LinkedIn, etc.);
 - Blogging and other on-line journals and diaries, bulletin boards and chat rooms;
 - Microblogging such as Twitter;
 - Postings of video or audio on media-sharing sites such as YouTube.

SN Policy Structure

Applicability

- This policy applies to Social Media Activity whether the employee is on or off duty, whether the employee is using Company or personal electronic resources, and whether or not the employee posts anonymously or is using a pseudonym.

Guidelines

- Access to most social media networks through the Company internet has been granted as a useful business tool so that employees may view Company information.
- Employees are expected to limit personal use in accordance with the Company Integrity Standard on proper use of corporate assets.
- Employees may occasionally access non-business related pages so long as such use does not interfere with the employee's job performance, or with the security or effectiveness of any system. Employees should have no expectations of a right to privacy regarding their Social Media Activity.

SN Policy Structure

Workplace Concerns

- If employees have concerns about their workplace, they are encouraged to resolve such issues by speaking directly with their supervisor, co-workers, Human Resources, or other Corporate resource rather than using Social Media Activity.

Enforcement

- The Company may, at its discretion, review Social Media Activity that impacts the Company, its employees, customers or vendors to the fullest extent permitted by law.
- If an employee engages in Social Media Activity anonymously or using a pseudonym, the Company may, in appropriate circumstances, take steps to determine identity.
- Employees will be held accountable for engaging in Social Media Activity that violates this policy or any other applicable policy. Failure to comply with the policy may result in disciplinary action up to and including termination, legal action and/or criminal prosecution.
- The Company will not construe or apply this policy in a manner that improperly interferes with or limits employees' rights under the National Labor Relations Act, or any other applicable law.

SN Policy Should Cover

- **Which sites employees can access**
- **You can log into a personal account of an employee**
- **If an employee can:**
 - **join Social Networking sites using their corporate e-mail**
 - **solicit others in the company to connect**
 - **recommend others on LinkedIn and other SN sites**
- **You can monitor what employees say / post**
 - **From work**
 - **From home**

SN Policy Should Cover

- **Use of SN sites to perform background checks**
 - Beware of exposure to protected data, illegal access to the data, false positives or wrong identity
 - Need to avoid claims of invasion of privacy or improper reliance on off-duty activity
- **Use of SN sites to look for talent**
 - Many of the same concerns arise

Enterprise Guidance

Members engage in public discourse in a responsible and respectful manner

Comply with corporate policies and procedures to ensure the security and privacy of our customers' data

Be aware of this responsibility when using public social media

Only those officially authorized can speak publicly on behalf of the enterprise, including press releases, interviews, and other public statements

Enterprise Guidance

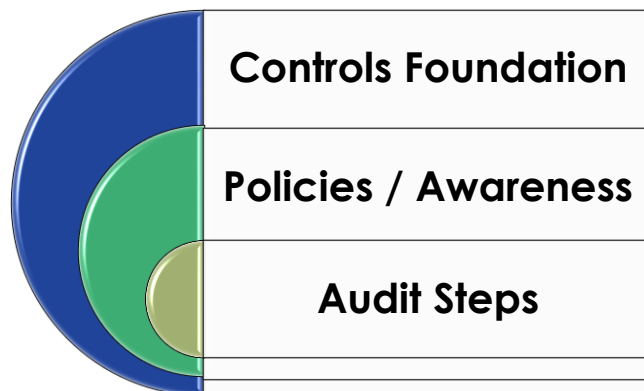
Only those officially approved by the **Social Media Governance** team may provide service or promotional statements via our social networking sites

Access to enterprise's social networking sites must be properly reviewed, authorized, and granted

Access will only be authorized for a legitimate business need and will be granted at the "minimum level necessary"

If you identify yourself as an employee of the enterprise, note the opinions are yours and not necessarily those of the company

Audit and Control Implications



Audit Objective

To provide management with an independent assessment relating to the effectiveness of controls over the enterprise's social media policies, program and processes

Basic Audit Steps

Strategy

Has it been defined

How has it been communicated

Has it been consistently applied

Tools

What tools are being used

By whom and when

Rules of Engagement

Employee guidelines

Employee training

Policies and procedures

Subsidiaries

Control Tools

Proper Tools

SM Management Platform

SM Listening Platform

SM Archiving Platform

SM Compliance Tool

Basic Audit Review

Identify related technology in place

Determine if a risk assessment was done and risks mapped with various regulatory and compliance requirements

Determine if monitoring of sites and content has been established

Determine if cost benefit and feasibility was performed

Determine if a formal incident response plan exists and it updated

Educate employees on policy, security and privacy issues

Identify the social media tools

Determine existence of Policies & Procedures

Determine if there are 3rd parties involved and the SLAs

Basic Audit Steps

Determine existence of social media governance framework: leadership / accountability, policies / guidance, stakeholder involvement

Determine who can update the site content who approves the content

Determine who is monitoring the websites and if there is a process for responding to social media threats

Determine if processes been established for creation and management of social media channels

Determine if these are scanned for vulnerabilities

Determine if there is an information management strategy to integrate social media content

Determine if social media information has been included in the data classification process

Determine if antivirus software is implemented with the appropriate settings to mitigate risk associated with social media

Key Audit Areas

Strategy

Governance and compliance

Processes

- Internal and external policies and program execution
- Metrics and monitoring
- Third party relationship management

People

- Training and awareness
- Recruiting and work force management

Technology

- Information systems operations
- Network management
- Third party management
- Information security and privacy

Audit Questions: Strategy

- Is it led by an executive champion and adequately funded and staffed?
- Does it provide direction for all stakeholders?
- Does it define social media program model and define target audiences and channels?
- Is it aligned with business objectives and other strategies?
- How often is the strategy updated / reviewed?
- Does it identify metrics to measure effectiveness?
- Is it pervasive and integrated throughout the business?

Audit Questions: Governance

- Does it define appropriate policies for social media?
- Does it establish social media program oversight responsibility:
 - board-level awareness and qualified program champion
 - effective oversight for all SM use / program monitoring / reporting
- Does it balance risks and opportunities?
- Does it include effective oversight for social media use:
 - Management awareness and monitoring,
 - Responses to social media event

Audit Questions: Governance

- Does it identify all relevant laws and regulations: Local and global, PCI and other relevant standards?
- Does it recognize how social media increases compliance efforts?
- Does it extend compliance, supervision and surveillance practices to interactive content?
- Does it monitor social media use for violations?
- Does it monitor compliance environment for potential changes related to social media?
- Does it include guidance for collecting and archiving social media content and activities (e-discovery)?

Audit Questions: Policy

- Is it aligned with business objectives, culture and core values and cover both internal and external personnel?
- Does it define platforms, formats and tools used to support social media and social media initiatives, including crisis communication?
- Does it outline monitoring practices for social media conversations, information collected, competition monitoring, and reputational risk monitoring?
- Does it define management reporting?
- Is it vetted by key players throughout the organization, including subsidiaries?

Audit Questions: Metrics

Do they provide insight into success and failure of social media activities?

Are they aligned with business objectives?

Are metrics consistent across business units and shared with business units and social media champion?

Are metrics defined for each social media initiative?

Are both qualitative and quantitative measures used?

Do metrics support regulatory compliance requirements?

Audit Questions: 3rd Party Management

Does it recognize all relevant content may not be in control of the social media program?

Does it include cross-functional review of contracts for social media relevance?

Does it provide guidance on how contracts and agreements affect organization's operations, risk and compliance positions?

Does it include risk assessments for third parties?

Does it address requirements for records retention?

Audit Questions: Training

Is it required for new hires and at least annually and offered enterprise-wide?

Does it incorporate awareness campaigns and include additional training for core social media team?

Does it cover: social media roles, responsibilities and expectations especially for crisis communications?

Does it identify the level of representation for the company and relevant policies and best practices?

Does it cover social media rules of the road, social engineering, security, privacy and data protection?

Does it ensure the legal and compliance processes are streamlined for SM?

Audit Questions: Technical

Are there monitors for:

Malware and viruses

Data leakage/theft

Owned systems (zombies)

System downtime

Recovery resources

Brand hijacking

Customer backlash/adverse legal reaction

Data exposure

Reputation

Targeted phishing

Audit – Things to Look For

- The authorizations granted to staff who manage the SN sites adheres to the minimum necessary rule
- The company properly limited direct access to SN accounts to the smallest group possible
- Practicing proper password protocols
- Regularly scan for unauthorized / fraudulent SN accounts
- SN posting procedures are being observed
- Existence and testing of a SN incident response plan
- Messages posted comply with policy (content and process)
- Listening and responding to what is said on SN

Agenda

- What it is & How it is used
- Survey Results
- Various Issues
- Audit & Control Implications
- ➔ Risk Mitigation
- Sample Audit Findings

Where are the Risks?



Employee and third-party access through a company network



Employee and third-party access on private networks



Communication with customers/constituents over social channels

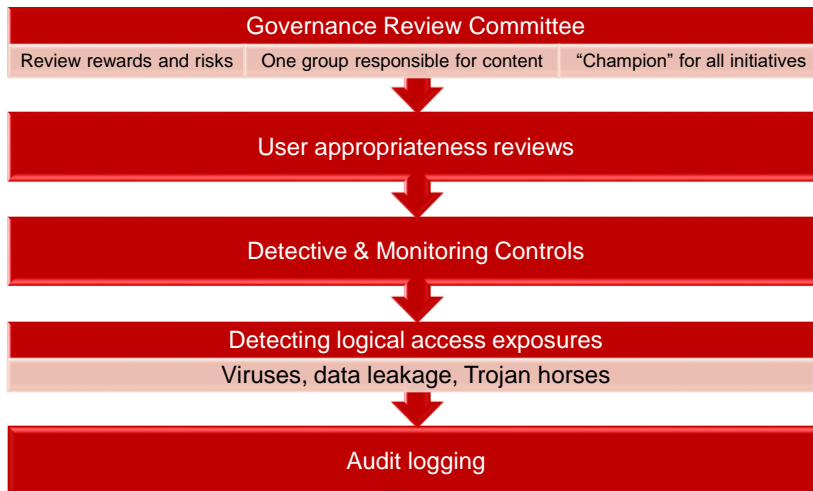


Public forum discussions about your company, products and services



Management of rapidly evolving technologies outside the company's direct control

Risk Mitigation




Risk Mitigation

- Develop awareness
- Implement Policies and Procedures
- Educate yourself, staff and members
- Engage associates
- Strong password management

Risk Mitigation

- Communicate expectations
- Monitor what is said
- Manage the process
- Prepare a contingency plan
- Involve Privacy & Security early


Simple Guidelines



- **Explicitly explain what you can and cannot talk about.**



- **No anonymous posting!**



- **Make it clear: “you write it, you own it.”**


Simple Guidelines



- **Adjust guidelines due to your industry, culture, etc.**



- **Reserve the right to remove any comments or posts.**



- **Violations may result in disciplinary action, up to and including termination.**

Agenda

- What it is & How it is used
- Survey Results
- Various Risks / Issues
- Audit & Control Implications
- Risk Mitigation
- Sample Audit Findings

Potential Audit Findings

- Finding #1 Governance**
 - There is no central group responsible for SN governance
 - The results of social media activities are not being reported to the appropriate level
- Finding #2 Strategy**
 - Overall strategy has not been articulated
 - Strategy is not aligned with the organization's objectives
 - Strategy is not reviewed and updated
- Finding #3 Plan**
 - SMART goals have not been established
 - Goals are not monitored and reviewed

Potential Audit Findings

Finding #4 Governance

- Roles and responsibilities have not been defined for all individuals involved in social media projects
- Lack of coordination between various projects

Finding #5 Metrics

- Metrics:
 - have not been established to determine value of the SN
 - do not align to company goals
 - are not reviewed and actioned

Finding #6 Monitoring

- There is no process to identify issues / concerns
- Escalation protocols have not been established for issues / public relations concerns

Potential Audit Findings

Finding #7 Training

- Awareness training do not exist
- Lack of internal websites for dissemination of information

Finding #8 Policies

- Policies have not been created and / or updated
- Employees are not aware of the policies
- Policies are not adequate and specific

Finding #9 Regulatory

- No one responsible for regulatory review
- No one ensuring law changes no not affect SN protocols

Next Steps

Users share information inappropriately, putting their identities – and your firm – at risk

Educate workforce regarding online risks

Need to offer greater security and control to social networkers

Regularly review the information you and your staff are sharing online, and act as appropriate

Review your web 2.0 security settings – you should only be sharing info with trusted parties

Consider filtering access to social networks –groups and time

Scan websites accessed for malware/cybercrime

In Conclusion



Risks are real and as yet not fully defined

- May be greater or less than anticipated



Companies can and should prepare

- Understand the risks for your business and educate workforce to risks
- Develop policies, if needed, and keep them current



Think about the new generation

- Has different notion of private and public
- May be better to embrace and channel the drive
- Expect many things to be different in the months ahead