

Powerful Insights. Proven Delivery.®



Guidance Through Powerful Insights

Emerging Technology and Security Update

*Presented by, Cal Slemph
Managing Director, New York, NY*

October 25, 2012

protiviti®
Risk & Business Consulting.
Internal Audit.

Speaker



Presenter

Cal Slemp

Managing Director, New York

Topic

Emerging Technology and Security Update

Objective

Provide:

- An overview of and key risks associated with cloud computing
- If time allows, also address security considerations with Social Media

Relevant
Experience

- Protiviti's Global Leader Security and Privacy Solutions
- Associated with IBM for 30 years prior to joining Protiviti, led their global Security and Privacy Services team
- Developed a unique identity management service offering for IBM called Trusted Identity



Framing the Discussion

Emerging IT Trends



Demand Side

1

Rise of the Knowledge Worker

Widespread transaction automation and outsourcing, and the resulting shift in retained skills, mean almost everyone is becoming a knowledge worker

2

Ubiquitous Data

The rise of "smart" mobile devices and "ubiquitous sensing" will drive an exponential increase in data volume and throughput

3

Social Media

The way customers and consumers learn about products and interact with companies is changing fundamentally

4

Emerging Market Growth

Shifting global demand means emerging markets will be main source of growth, eventually reaching the scale of developed markets

5

Efficiency Shortfalls

The corporate center (IT, Finance, HR, Supply Chain, Procurement, etc.) is reaching the limits of efficiency in its current functionally-oriented form

6

Tech-Savvy Workforce

Technology knowledge and confidence in the workforce is broadening but losing its depth (fewer have a deep technical expertise)

Important but not Transformative trends

7

Green IT

Green IT, greater government intervention in the economy

Source: CIO.com

Emerging IT Trends (cont.)



Supply Side

8

Technology as a Service

Infrastructure and applications are becoming available as virtualized, configurable, and scalable services in the cloud (or will) adopt licensing structures to mimic a service

9

The Industrialized, Externalized Back Office

Industry standards will emerge for back-office business processes that are then delivered by external providers

10

A Blueprint for Service Delivery

ITILv3 provides a pathway to reorienting IT around service delivery

11

Desktop Transformation

Virtualization, SaaS, and unified communications combined with greater workforce mobility triggers a "transformation of the desktop," enabling device-agnostic service delivery

Organization Side

12

Fewer than 25% of employees currently within IT will remain in their current roles

13

Many activities will devolve to business units, be consolidated with other central functions such as HR and finance, or be externally sourced

14

CIOs face the choice of expanding to lead a business shared service group, or seeing their position shrink to managing technology delivery

15

Several trends in IT demand and supply will change how organizations use technology to create value, and the roles, structure and skills of the IT function

Source: CIO.com

Emerging Strategic Technologies



Gartner defines a strategic technology as one with the potential for significant impact on the enterprise in the next three years. The following are the top technologies that could have a potential impact on future strategic direction which businesses may chose to take.



Cloud
Computing



Social
Media



Green IT



Internet
Marketing



Mobile
Commerce



Context
Aware
Computing



Off shoring
/ Out
sourcing



IT Security

IT Capabilities and Needs Insight



Table 1: Overall Results, Technical Knowledge

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency (5-pt. scale)
1 (tie)	Virtualization	3.1
	Social Media Integration	2.8
3	Cloud Computing	3.0
4	Social Media Security	2.6
5	Mobile Commerce Security	2.4
6	NIST (cybersecurity)	2.4
7	Data Breach and Privacy Laws (various U.S. states)	2.7
8	Mobile Commerce Integration	2.5
9 (tie)	CISSP	2.7
	Mobile Commerce Policy	2.4
	CISSA	1.2
	Smart Device Integration	2.5








Multiple Models of Cloud Computing

Cloud computing is a model for enabling on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

OR more simply,

“IT runs over the Internet instead of installing hardware and software yourself.”

Characteristics

	On demand self-service
	Pay as you use
	Rapid elasticity (expand / contract)
	Multi tenancy (shared pool)
	Broad network access

Service Models

Business Process as a Service (emerging) Entire business process as a service in the cloud
Software as a Service Finished applications that you rent and customize
Platform as a Service Developer platform that abstracts the infrastructure, OS, and middleware for developer productivity
Infrastructure as a Service Deployment platform that abstracts the infrastructure

Deployment Models

Public Cloud
Community Cloud
Hybrid Cloud
Private Cloud

How Can It Help Businesses?

- Serving High Demand
- Allowing High Variable Demand
- Reaching Geographically Dispersed Users
- Assisting with Start Ups
- Consolidating Company IT
- Experimenting Easily and Cheaply
- Planning for Disaster Recovery
- Operational Expertise – Patch Management, Version Updates, Data Security Management





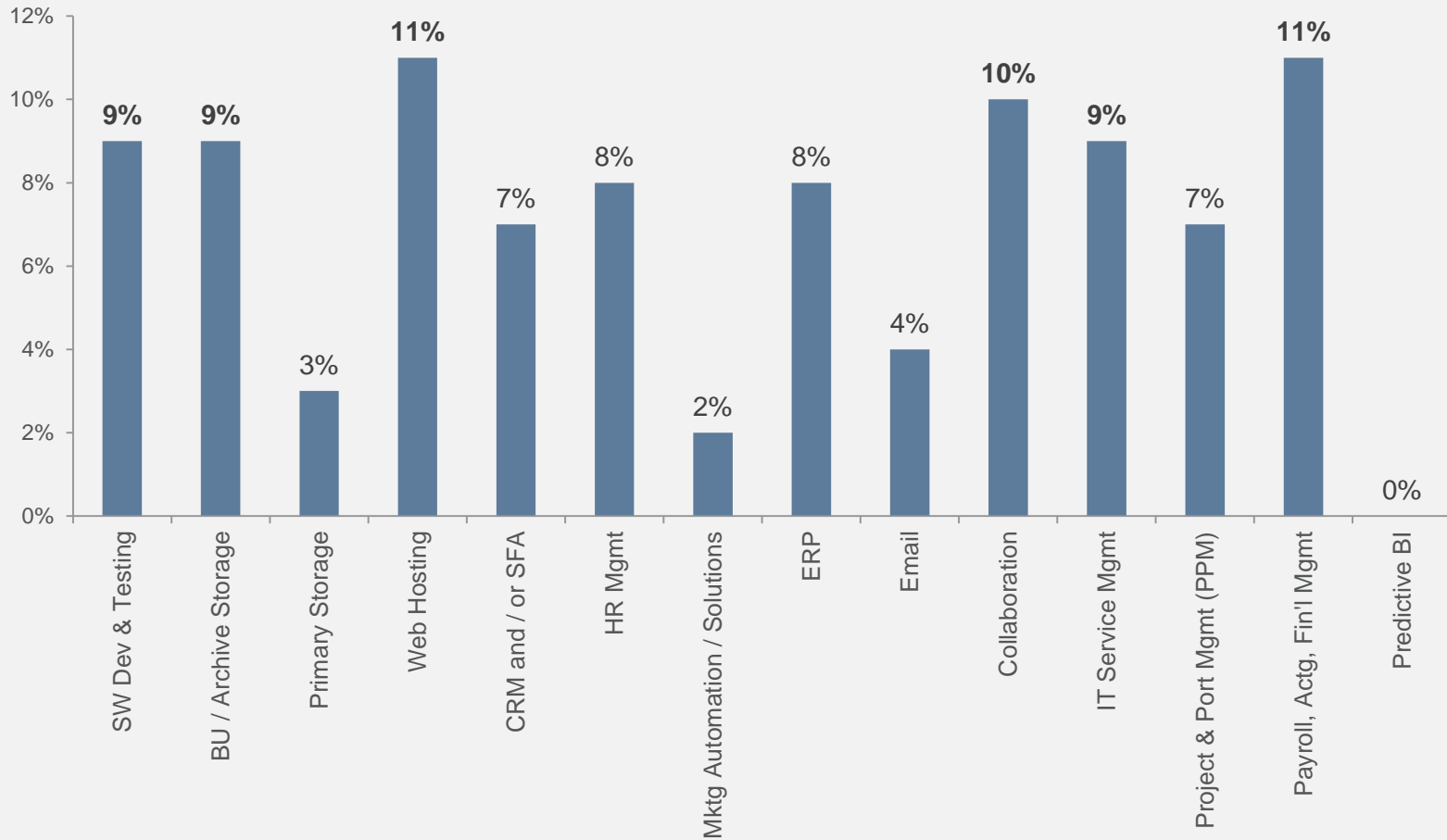
Many Cloud Computing Offerings



** A sample list only. There are many more players.*

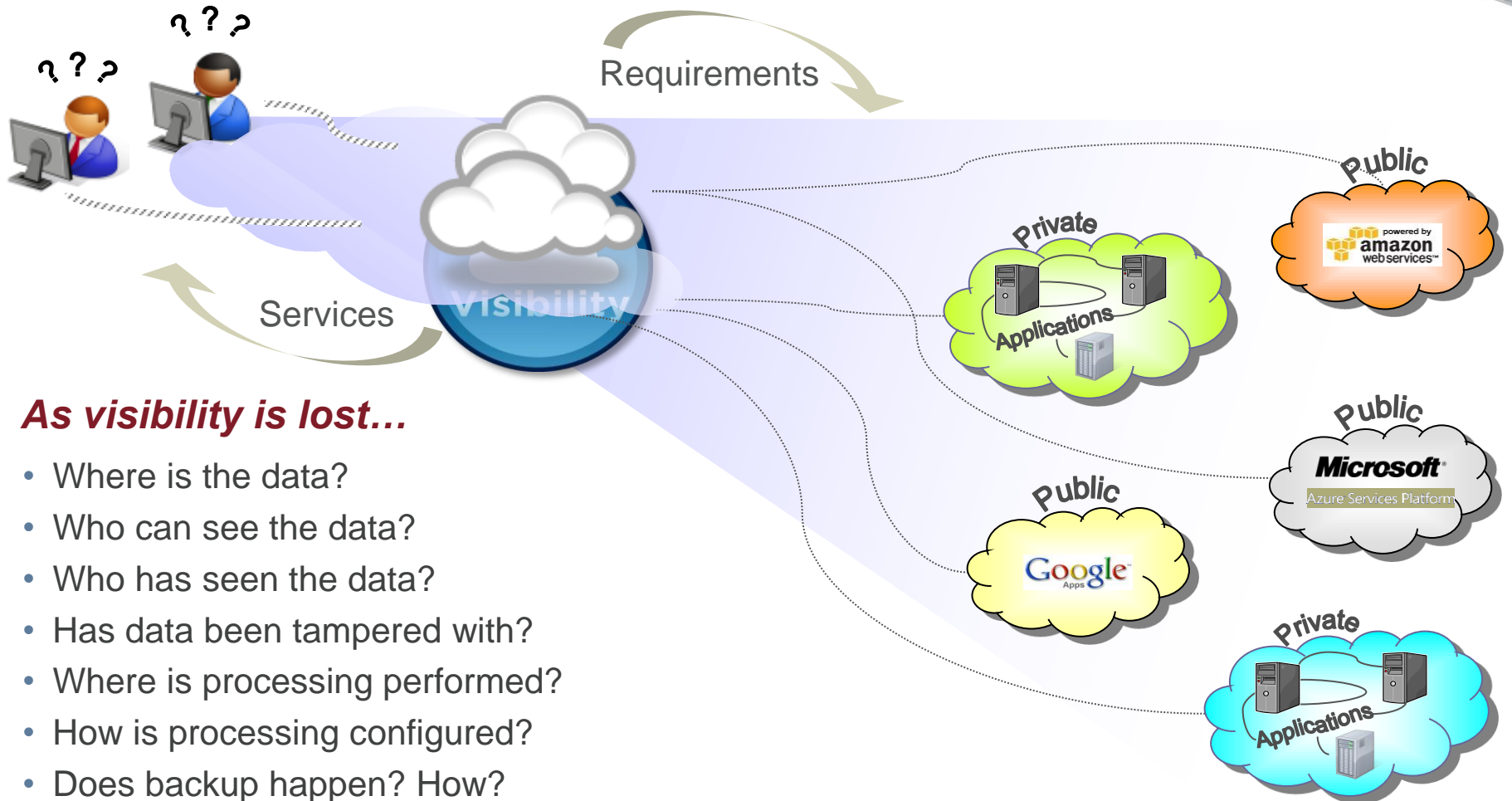


How The Cloud Is Being Utilized ?



Source: March 2011, Worldwide Executive Council

Clouds Are Cloudy



As visibility is lost...

- Where is the data?
- Who can see the data?
- Who has seen the data?
- Has data been tampered with?
- Where is processing performed?
- How is processing configured?
- Does backup happen? How? Where?

... security, compliance, and value are lost as well.

Top Risks

Loss of Governance

Lock-In

Management Interface Compromise

Incomplete or Insecure Data Deletion

Data Protection

Malicious Insider

Isolation Failure

Compliance Risks



Categories of Control Objectives

Compliance

Data Governance

Facility Security

Human Resources

Information Security

Legal

Operations Management

Risk Management

Release Management

Resiliency



Control Objectives



Compliance	Independent Regulatory Audits
	Vendor Management
	Information System Regulatory Mapping
	Intellectual Property
Data Governance	Classification
	Handling / Labeling / Security Policy
	Retention Policy
	Risk Assessments
Facility	Policy
	User Access
	Asset Management
Human Resources	Background Screening
	Employment Agreements
	Employment Termination

Control Objectives



Information Security

Management Program

Policy, Reviews, Enforcement

User Access Restriction / Authorization / Reviews

Awareness Training

Roles / Responsibilities

Management Oversight

User Access Policy

Workspace Cleanliness

Anti-Virus / Malicious Software

Incident Management – Identification, Reporting and Monitoring

Incident Response Legal Preparation

Control Objectives



Legal	Non-Disclosure Agreements
	Third Party Agreements
	Service Level Agreements
Operations Management	Capacity / Resource Planning
Risk Management	Program
	Assessments
	Mitigation / Acceptance
	Business / Policy Change Impacts
	Third Party Access
Release Management	Production Changes
	Outsourced Development
Resiliency	Management Program
	Impact Analysis
	Business Continuity Planning
	Business Continuity Testing

Involvement of Internal Audit



Vendor Selection & Contract Negotiation

- Validation of business case
- Right to Audit Clause and / or SAS70 (SSAE16)
- Compliance Scope
- Impact of Regulations on Data Security
- Stability of Partners and Services Providers
- Contractual Data Protection Responsibilities and Related Clauses
- Impact of Regulations on Provider Infrastructure
- Prepare Evidence of How Each Requirement Is Being Met

Pre-Implementation Review

- Project management - roles and responsibilities
- Data migration strategy

Post-Implementation Review

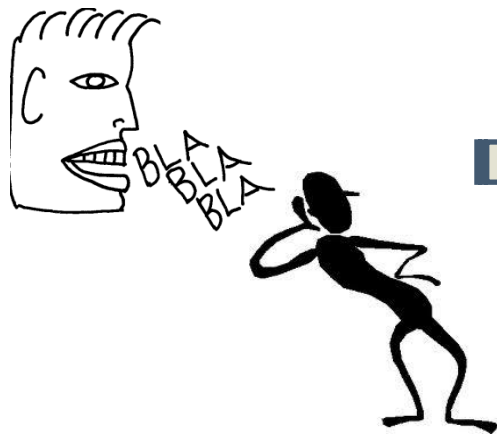
- Accuracy of data
- Policies and procedures pertaining to data security, privacy of data
- Regulatory changes - HIPAA, PCI, etc.



Social Media Considerations

What Is Social Media?

- Technologies that allow bi-directional communication among many participants
 - Evolution from uni-directional 1:1 and 1:many communication to **bi-directional many:many** interaction
 - Intended to drive **engagement**
 - Provides easy-to-use tools with a very **friendly user interface**
 - Mostly Internet-based (with implications on **speed and breadth** of communication)



SOCIAL MEDIA EXPLAINED

TWITTER I'M EATING A #DONUT

FACEBOOK I LIKE DONUTS

FOUR SQUARE THIS IS WHERE
I EAT DONUTS

INSTAGRAM HERE'S A VINTAGE
PHOTO OF MY DONUT

YOU TUBE HERE I AM EATING A DONUT

LINKED IN MY SKILLS INCLUDE DONUT EATING

PINTEREST HERE'S A DONUT RECIPE

LAST FM NOW LISTENING TO "DONUTS"

G+ I'M A GOOGLE EMPLOYEE
WHO EATS DONUTS.



Security Trends in Social Media

- **21%** accept contact offerings from members they don't recognize
- **More than half** let acquaintances or roommates access social networks on their machines
- **64%** click on links offered by community members or contacts
- **26%** share files within social networks
- **20%** have experienced identity theft
- **47%** have been victims of malware infections
- Facebook has been hit with malicious applications and new version of the Koobface virus, which allows hackers to steal information from personal profiles
- Huge increase in “likejacking”



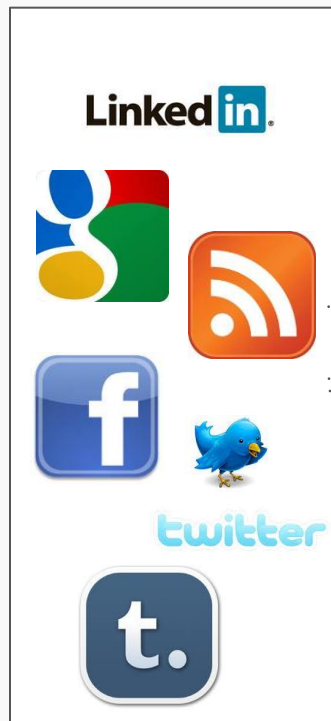
<http://www.webpronews.com>

Social Use Cases and Key Risks



Uses

Risks



Other Risk Considerations



Financial Risk



Remarks about company performance could impact stock price and performance. (“The strategic plan for Company C is not going to work and results are not going to be good...”)

Safety Risk



Release of information about what someone is doing or where someone is traveling. (“Our executive team is meeting at Location Z...”)

Personal Reputation Loss



Remarks made by an individual or friends of an individual could be viewed by others (“I can’t believe what happened the other night when I was out for dinner...”)

Other Risk Considerations (cont.)



Metrics Integrity Risk



Metrics used to measure results of social media efforts may be invalid or inappropriately measured leading to poor decisions and investments.

Litigation Risk



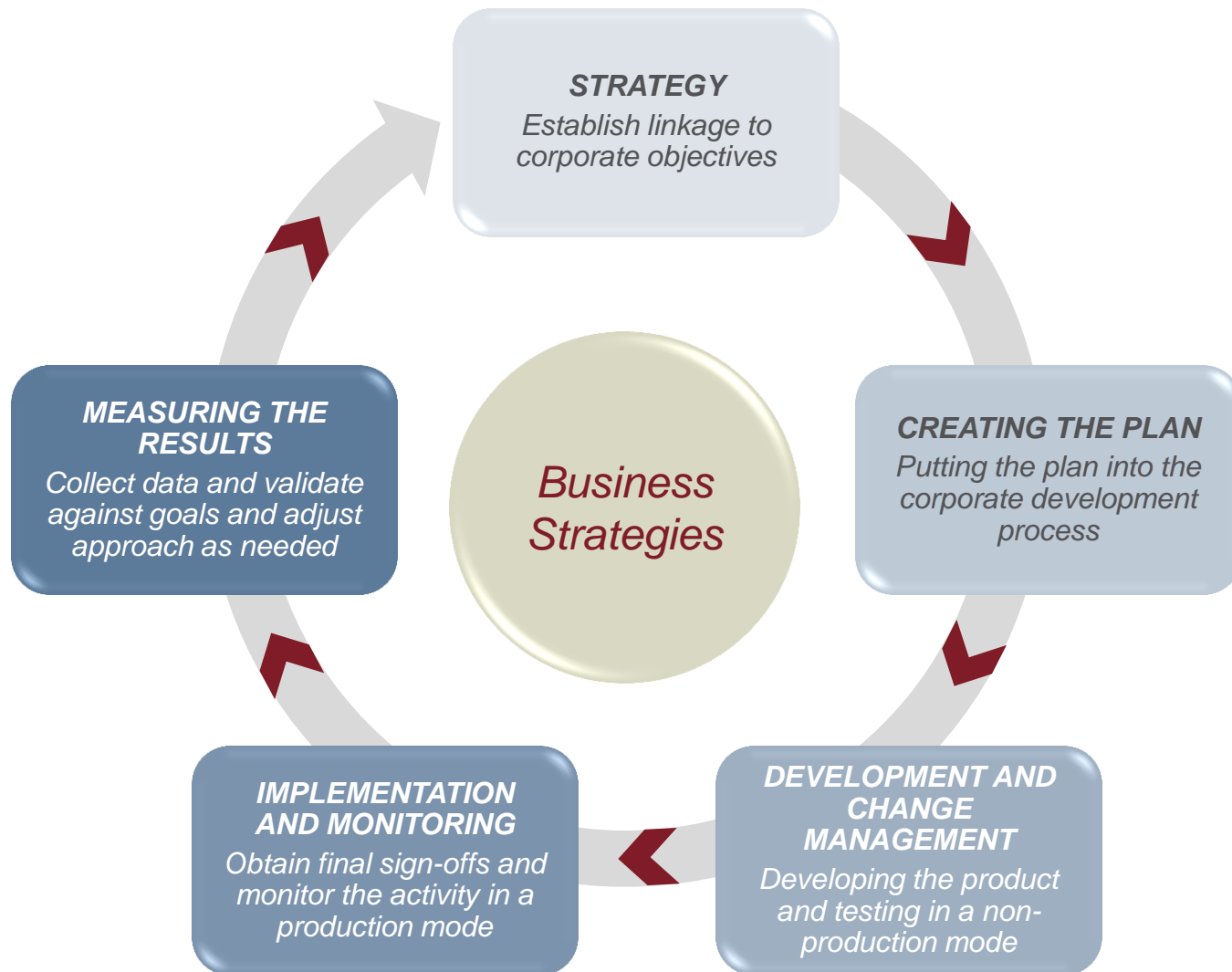
What is said on social media sites can, and will, be used against individuals and companies in a court of law.

Lack of Governance



Appropriate involvement of stakeholders and executive oversight do not correlate social media activities to company objectives and culture.

The Social Media Lifecycle



The Social Media Lifecycle

Guiding Principles



Governance

- Ensure that the social media capabilities have appropriate oversight and ownership
- Coordinate/integrate social media efforts with other marketing activities
- Monitor market developments with emerging social media offerings
- Establish appropriate review and quality assurance steps

Capabilities

- Review current skill sets within the organization and validate what may be needed to deliver social media efforts. Introductory and “expert usage” training is essential.
- Make sure that the IT organization is appropriately involved for evaluation and consideration of social media designs

Integrity

- Establish an environment where capabilities can be developed with appropriate oversight and security. Reinforce with clear policies and procedures.
- Design appropriate monitoring oversight for development and production environments
- Review interaction of social media capabilities with existing systems and business processes
- Validate risks and ongoing monitoring steps

Security

- Validate security design
- Ensure appropriate access to development and production environments
- Review and implement automated tools to support security monitoring
- Integrate with your existing security and privacy practices

Some Useful Information Sources



Auditing Social Media – A Governance and Risk Guide - www.theiia.org

Social Media Audit / Assurance Program - www.isaca.org

Social Media Governance - www.socialmediagovernance.com/policies.php

Social Media Explorer - www.socialmediaexplorer.com



Risk & Business Consulting
Internal Audit



Social Media and Internet Policy and Procedure Failure – What's Next?

POWERFUL INSIGHTS

With the widespread adoption of social media by employees and within business operations, risk management professionals continue to establish a set of policies and procedures to guide social media usage. Companies are envisioning stages of establishing training awareness programs to ensure that employees understand what constitutes legitimate conduct and what would be deemed as violations. With the evolution of more sophisticated monitoring products, companies now have an opportunity to evaluate employee social media usage both before and within the confines of corporate networks and infrastructure. However, a recent statement in a high profile case has sent companies back to the drawing board to re-evaluate their social media and internet policies and procedure.

Issue

A Connecticut based corporation fired an employee for posting negative feedback about a supervisor on her Facebook page. The language in the policy established by the company prohibited employees from making disparaging, discriminatory, or defamatory comments when discussing the company or the employee's supervisor, coworkers, and/or competitors.¹ The National Labor Relations Board (NLRB) filed a complaint alleging that the employee's fired violated federal labor law because she was engaged in protected activities before the posting of the comments, and that the employee was illegally denied union representation during an investigation. Based on the NLRB's action, the company agreed to waive its corporate policies, which had been deemed by the NLRB to restrict employees' rights and also to prevent the employee from discussing other topics such as wages, hours and working conditions.

Because of this action, companies are being challenged to ask whether their policies violate the rights of employees and potentially can be deemed as being in violation of the National Labor Relations Act, which not only applies to employed labor, but also to all private employers in the United States.

Challenges and Opportunities

Companies need to take a step back and evaluate what social media and internet policies mean for their specific and unique business operations and culture. Some companies are in the process of putting in place a firmly established set of policies, have revised examples of other company policies, have retained that examples of other company policies and internet policies exist at their own, without giving thought to employees use (misuse) and potential for abuse. This is not a prudent approach. When talking to stakeholders, internal and external, and legal policies for social media and internet usage, the adage "we do it so we don't do it" is highly applicable.


An organization needs to find the right balance of language and direction in their policies; they also need to be transparent to how they will be monitoring for compliance and what constitutes a violation and potential outcome when such internet occur.

Finally, companies need to engage their employees in the process to better understand what social media capabilities may be cited and the reasons why these capabilities may be desirable not only from an individual employee's perspective, but also for the company's overall benefit.


Our Point of View

The implementation of social media and internet usage policies should be a measured (flexible) process that incorporates thoughtful use of key decision-makers within the company and external experts (e.g., legal counsel) and potential violations situations concerning implemented policies. More specifically, companies should consider the following:

- Determine the goals and objectives of the social media capabilities as linked to corporate objectives and key initiatives.
- Determine how employees may want to leverage social media to engage with customers and prospects.
- Understand how social media capabilities will support meet other marketing capabilities.
- Establish metrics for measuring the achievement of goals/objectives established for the social media capabilities.



Risk & Business Consulting
Internal Audit



IT Auditing – Expanding Scope to Encompass Social Media

POWERFUL INSIGHTS

Issue

Social media is not only becoming a part of everyday business operations, but also a competitive necessity. Yet in many organizations, the potential risks related to employee use of social networking sites, as well as tools and technologies for communication and collaboration, are not closely monitored or fully assessed by internal auditing teams. In fact, a recent Knowledge@Wharton survey revealed that 53 percent of organizations did not even include the evaluation of social media risks in their 2011 audit plans.¹

One reason many firms have not made assessing social media-related risks a priority is the perception that social media risks could be the foundation of company policies and enforceable actions. As a result, even IT auditors – those responsible for reviewing risks related to IT systems and processes and assessing the effectiveness of information security and other IT strategies, policies and practices – typically do not view social media as an area that should be risk assessed annually and audited as necessary. However, given the risks involved, this attitude must change.

Challenges and Opportunities

Social media presents an array of significant risks to the enterprise. In addition to the potential loss of intellectual property, which could undermine an organization's competitive edge, and the communication of sensitive data to unauthorized parties, which could result in costly compliance violations, improper use of social media could lead to:

- **Reputation risk** – Stakeholder remarks and comments posted on social networking sites by disgruntled workers, clients or customers can damage the firm's image significantly and can impact the firm's ability to attract and retain business.
- **Internal control risk** – There also is the risk of an accidental reputation damage that can occur when, for example, a company employee posts a personal – and perhaps inappropriate – message on Twitter while signed on to the company's account instead of his personal one.

Financial risk – Remarks made in the "social sphere" about the company and its performance could affect stock price and performance.

Safety risk – Release of information through social media channels about what executives or other employees are doing or where they are traveling could put them at risk.

Loss of strategy – Strategies for using social media and ensuring they are well thought out and monitored so that organizational benefits from them need to be coordinated. Otherwise, they waste time and money on something that fails to increase customer loyalty and satisfaction or attract new customers.

Many of the potential risks to the enterprise that social media presents, whether related to IT security or marketing-related activities, are not new. Because of the rapid exchange of information occurring through social media channels and the vastly wider audience that may witness or feel the impact of a negative event, these risks must be taken seriously, and closely monitored, by businesses. For many organizations, if auditors will be at the forefront of efforts to monitor and manage these risks.

Our Point of View

Social media risk, like any risk, should be monitored and managed through training, awareness, policies and procedures, and with appropriate controls to test the effectiveness of these measures. Many enterprises already are monitoring a wide range of IT risks. They just need to expand their scope to include social media.

Also, access to social media is not only instantly instant, but available to a broad audience that includes clients, customers, shareholders and the public, as well as company personnel. These employees, in particular, may create inappropriate – message on Twitter while signed on to the company's account instead of his personal one.

Board Perspectives: Risk Oversight

Issue 29



Social Media: What It Means to Your Risk Profile

Social media is a compendium of many things – corporate blogs, video-sharing sites such as YouTube, social networking like Facebook, microblogging tools such as Twitter, among others – that leverage the power of Internet, Web 2.0 and mobile technologies to connect people. The convergence of these technologies is forever altering the dynamics of customer relationship management, marketing and corporate communications for many businesses.

Key Considerations

Business-to-people communications and social media peer groups have emerged as a new model for connecting with markets and customers efficiently. Companies ignore this model at their own risk. These mediums are fertile for innovation, requiring organizations to contribute value-added content and transparency in an environment where customers and other parties drive the dialogue. Organizations failing to harness the potential value of social networking run a risk of becoming laggards as they cede to competitors the ability to lead their products and services distinctly in the public eye, as well as obtain common improvements unified, using this unique venue.

Social media uses enable companies to listen to and learn from satisfied and dissatisfied customers regarding their ideas, experiences and knowledge, as well as offer them an opportunity to reach out and proactively respond to customer views and reactions. In addition, social media is providing opportunities to produce developments across its own roadmaps and obtain early

input from potential buyer groups on new products plans. Marketing can use messaging and learn what messages work best in almost real time. Companies can educate and inform customers by engaging them on many topics around product uses and applications. While these developments are presenting significant opportunities for companies to connect with their customers and others, they are creating a whole set of new issues. Following are 10 examples:

- **Loss of IP and sensitive data** – Inappropriate release, leakage or theft of information strategic to the company and exposure of company networks and systems to viruses and malware.
- **Compliance violations** – Communication of data that violates applicable laws and regulations, including infringement of trademarks and copyrights, data security issues, employment issues, violations of privacy rights, and mismanagement of electronic communications that may be impacted by retention regulations or e-discovery requirements.
- **Reputation loss** – Because customer opinions can spread quickly through social media, companies need effective crisis response plans. In addition, self-inflicted reputation damage may result from inappropriate employee behavior, using unapproved product or customer service experiences, negative or disparaging messages intended for internal or personal use, or inability to measure up to the openness, honesty and transparency expected by customers and prospects.

protiviti.com



Wrap-Up

Call to Action



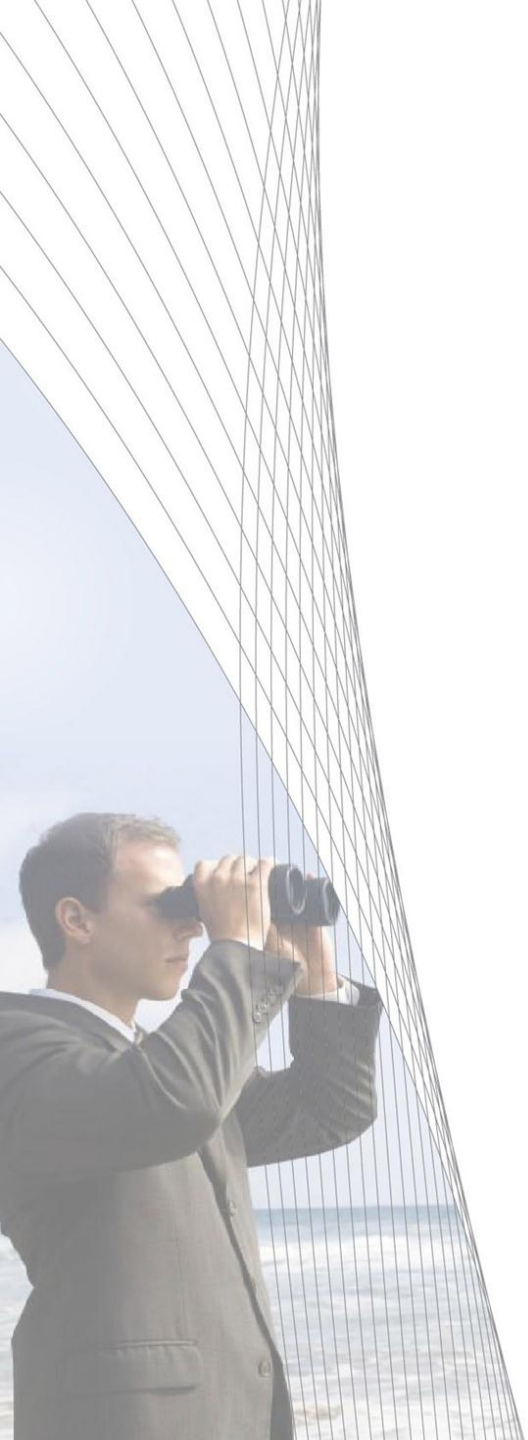
- Stay connected to corporate strategies and objectives and then anticipate their implications to the IT environment.
- Ensure the risks are articulated.
- Get involved with proof-of-concept activities for new capabilities and technology.
- Don't assume policies exist (or can be adapted) for adoption of new technologies.
- Make sure that appropriate and on-going training is in place to educate employees and also external customers.
- In coordination with the IT team, evaluate monitoring tools that can help address the risks of the emerging technologies.
- Ensure there is program and project management offices for emerging technology introduction and usage as well as the tracking of risks/issues and ROI.
- Review the support structure and organization in place to deal with internal and external customers.

*Powerful Insights.
Proven Delivery.®*

Q & A



protiviti®



Thank You



Cal Slem
Managing Director
New York, NY
+1.203.905.2926
cal.slem@protiviti.com

cal.slem@protiviti.com
+1.203.905.2926