



Borderless security

Annual Almost Free Seminar

21 June 2011

Agenda

- ▶ 2010 GISS Survey Observations
- ▶ Virtualization
- ▶ Cloud Computing
 - ▶ Industry Trends
 - ▶ SOC 2 and Cloud Computing
- ▶ Mobile Devices
- ▶ Social Media
- ▶ Contact Information

Section 1

▶ 2010 Global Information Security
Survey Observations

GISS Survey Observations

Borderless security

- ▶ 60% of respondents perceived an increase in the level of risk they face due to the use of social networking, cloud computing and personal devices in the enterprise.
- ▶ 46% of respondents indicated that their annual investment in information security is increasing, with only 6% planning to reduce their information security investment.

Mobile computing

- ▶ 53% of respondents indicated that increased workforce mobility is a significant or considerable challenge to effectively delivering their information security initiatives.
- ▶ 64% of respondents indicated that data (i.e., disclosure of sensitive data) was one of their top five areas of IT risk.
- ▶ 50% of respondents plan on spending more over the next year on data leakage/data loss prevention technologies and processes.
- ▶ 39% of respondents are making policy adjustments to address the potential new or increased risks.

Cloud computing

- ▶ 45% of respondents are currently using, evaluating or planning to use cloud computing services within the next 12 months.
- ▶ 54% of respondents who use cloud computing services indicated that they are using private clouds.
- ▶ 39% of respondents cited the loss of visibility of what happens to company data as an increasing risk when using cloud-based solutions.
- ▶ 85% of respondents indicated that external certification would increase their trust in cloud computing.

Social media

- ▶ Only 10% of respondents indicated that examining new and emerging IT trends was a very important activity for the information security function to perform.
- ▶ 34% of respondents include information updates on the risks associated with social networking.
- ▶ 45% of respondents indicated that they restrict or prohibit the use of instant messaging or email for sensitive data.

Section 2

▶ Virtualization

Virtualization Benefits

Consolidate

- Increase utilization
- Reduce hardware costs
- Save on maintenance and leases
- Save on energy costs
- Save on real estate

Manage

- Enhance IT Agility
- Accelerate provisioning time
- Manage heterogeneous systems from central point of control
- Establish shared infrastructure with resource pools

Automate

- Increase growth ability
- Enhance DR business resumption capability
- Eliminate repetitive maintenance and configuration tasks
- Maximize efficiency and responsiveness of data center
- Deliver critical services on -demand

Translate Servers to a *Collection of Manageable Resource Pools*

MANAGEMENT SERVICE

Manage
[Single Point of Control]

Virtual Machines

Application

Application

OS

OS

Virtual Machines

Application

Application

OS

OS

Virtual Machines

Application

Application

OS

OS

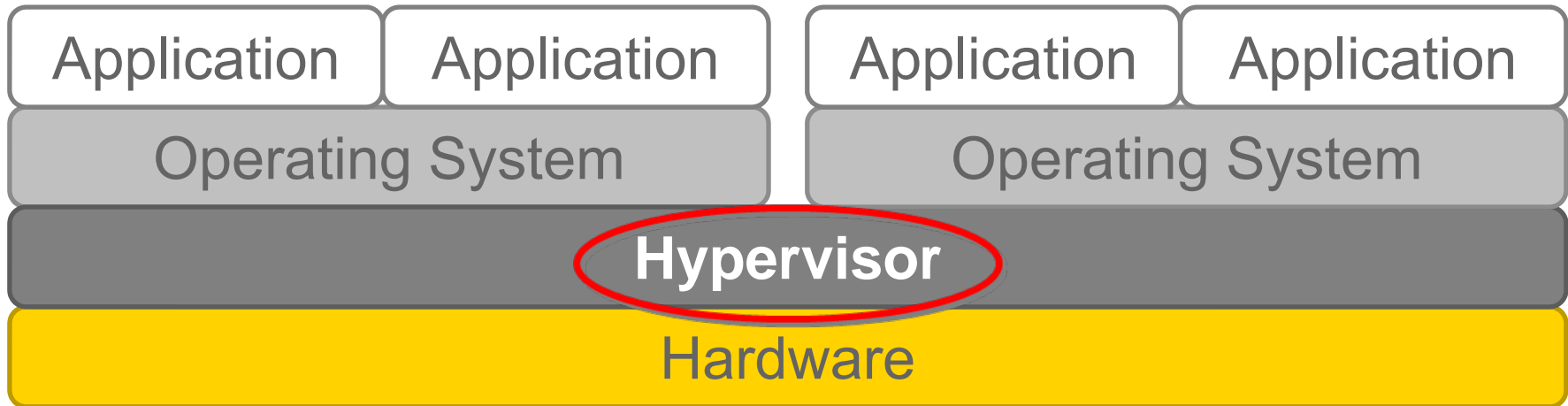
Virtualize



Virtualization Security Concerns

New number of security defects >
[Existing vulnerabilities
X
increased number of instances]

Virtualization Security Concerns



- ▶ The Hypervisor's attack surface is additive to the current risk profile.
- ▶ Flaws within inter-VM communication
- ▶ Separation of administrative duties: VM Hypervisor administrator has "keys to the kingdom"
- ▶ Virtual Machine Escape

Virtualization Security Concerns

- ▶ Limited view into the OS and virtual network to perform assessments – immature and incomplete assessment and management tools
- ▶ Not enough attention (yet) has been paid to patching virtualized environments
- ▶ Current security products may not work, most have not matured to leverage possible advantages of virtualization
- ▶ Virtualization security can impact performance, decrease value
- ▶ Security spend in a virtualized environment may be greater
- ▶ Data leakage through offline images

Section 3

▶ Cloud Industry trends

Three categories of Cloud Computing



Software as a service (SaaS)

SaaS refers to the ongoing support of applications whose core value to the customer pertains to alleviating the maintenance and daily technical operation and support of business and consumer software. (Salesforce.com)



Platform as a service (PaaS)

PaaS makes all of the facilities required to support the end-to-end life cycle of building and delivering web applications and services entirely available from the internet – with no software downloads or installation for developers, IT managers or end-users. It is also known as cloudware. (AWS, Rackspace, Hosting.com)



Infrastructure as a service (IaaS)

IaaS is a technology infrastructure delivery platform that is used to deliver software application environments. Customers no longer purchase servers, software, data center space or network equipment, but instead buy those resources as a fully outsourced service. (AWS, Rackspace, Hosting.com)

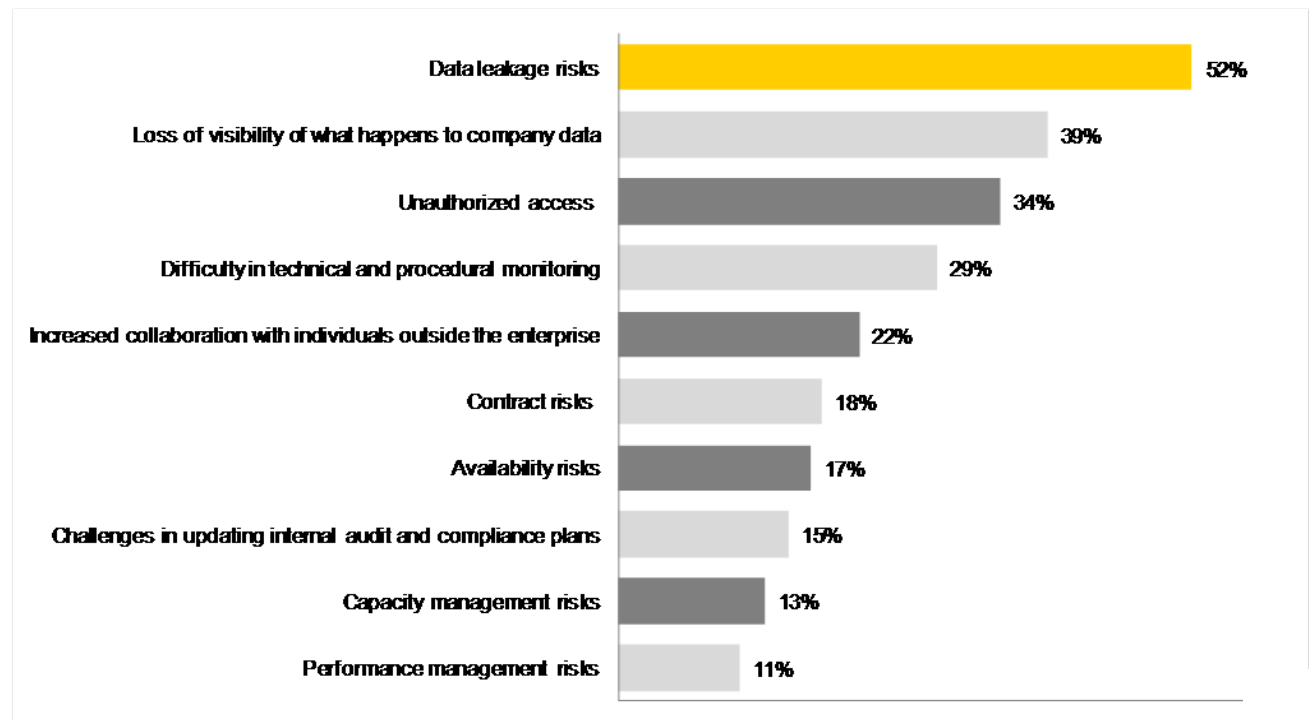
Industry trends

- ▶ **Comprehensive SLAs expected.** Infrastructure and platform providers are adopting aggressive service level agreements (SLAs) in an effort to differentiate their services in a space that is trending toward a commodity. What remains to be seen, however, is the stance that SaaS providers will adopt. Amazon is one of the few vendors that does offer an SLA. It is logical to assume that there will be some guaranteed service level for cloud vendors. More vendors are expected to begin offering comprehensive SLAs, especially as adoption grows in large enterprises.
- ▶ **Vertical blurring to continue.** Vendors have been moving both up- and downstream. Infrastructure providers such as Amazon have added development and database services to create a platform offering. On the other hand, a number of application providers have opened up their technology to allow third parties to develop programs on their architecture (e.g., VMware).
- ▶ **Rigorous vendor assessment processes.** Customers are continuing to mature their vendor assessment processes. These are continuing to have more focused attention on security given recent high profile data breaches at Epsilon, Sony, RSA and others. Security questionnaires and periodic audits of services providers are also increasing in frequency and depth.

2010 GISS results

Risks associated with cloud computing are not going undetected and must be addressed before business applications are moved to a public cloud

Which of the following “new” or increased risks have you identified?



39% of respondents cited the loss of visibility of what happens to company data as an increasing risk when using cloud based solutions.

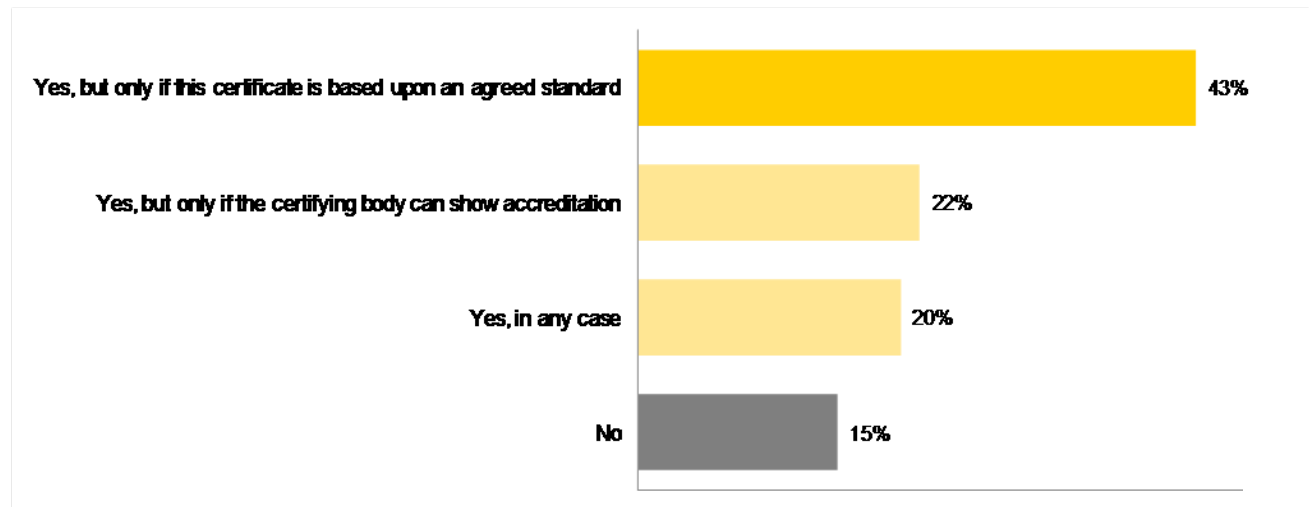
Note: multiple responses permitted
Shown: percentage of participants

2010 GISS results

Certification of cloud service providers would help in evaluating or confirming the appropriateness of security controls and increase trust

Would some kind of external certification of cloud service providers increase your trust in cloud computing?

85% of respondents indicated that external certification would increase their trust in cloud computing.



Shown: percentage of participants

Customer cloud computing considerations

What are the risks?

Privileged user access	Who at the cloud provider will have access to your data? What controls does the provider have over these peoples access? How does the provider hire and fire?
Regulatory compliance	How will using the cloud affect your ability to comply with regulatory requirements (e.g. SOX, GLBA, HIPAA, PCI)? Has the provider undergone any kind of third party audit or certification?
Data location and ownership	Where will the data be stored? Will it be replicated out of the country? Can the customer restrict where the data is stored? Who owns the data once it is in the Cloud?
Data segregation	How does the provider ensure that its other customers can not 'see' my data? What kind of encryption is in place? How are the keys managed?
Recovery	What happens to my data in the event of a disaster? Is it backed up or replicated somewhere else? How can I access my backups? How long does it take to restore my data?
Investigative support	If any kind of legal investigation is required because of illegal activity – can the provider support the customer to do the investigation?
Long-term viability	What sort of financial shape is the company in? Will they be around in the future? If the provider does fail – how can the customer get data back?

Security and Privacy Risks of Cloud Computing

- ▶ **Privileged user access**

- ▶ Increased need for verifiable provider controls and practices of how they hire and scrutinize privileged administrators who manage and protect data

- ▶ **Regulatory compliance**

- ▶ Customers are ultimately responsible for the security and privacy of their own data - even when it is held by a service provider
- ▶ Traditional service providers are subjected to external audits and security certifications
- ▶ Cloud computing providers refuse to permit this level of scrutiny which makes transparency impossible and would result in non-compliance

Security and Privacy Risks of Cloud Computing

▶ Data location

- ▶ Cloud customer typically do not know exactly where data is hosted - including what country it may be stored in
- ▶ While some providers may commit to storing and processing data in specific jurisdictions, customers need to confirm that their providers will make a contractual commitment to obey local privacy requirements

▶ Data segregation

- ▶ Data in the cloud is in a shared environment with data from other customers
- ▶ Customers need to understand how data is segregated at rest
- ▶ Encryption is effective, but isn't a cure-all
- ▶ Encryption accidents can make data totally unusable, and even normal encryption can complicate availability
- ▶ Cloud providers should provide evidence that encryption schemes were designed and tested by experienced specialists

Security and Privacy Risks of Cloud Computing

▶ Recovery

- ▶ Regardless of where your data is, a cloud provider should tell you what will happen to your data and service in the event of a disaster
- ▶ Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure
- ▶ Confirm , with contract SLAs, your provider has the ability to do a complete restoration, and how long it will take

▶ Long-term vendor viability

- ▶ Customers must be sure their data will remain available even if their providers fails or is acquired
- ▶ Providers should disclose how your data will be returned back and in a format that you could import into a replacement application

Security and Privacy Risks of Cloud Computing

▶ Investigative support

- ▶ Investigating inappropriate or illegal activity may be impossible in cloud computing
- ▶ Processing and enforcing legal hold orders may not be timely or reliable
- ▶ Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers
- ▶ Customers are typically unable to obtain contractual commitments to support specific forms of investigation and electronic discover (eDiscovery)
- ▶ Tracking physical location, modification or security features at an individual file level is not yet realized, but is a core requirement for eDiscovery

Section 4

▶ SOC 2 and Cloud Security

Independent assurance options to enhance service organization communications to its stakeholders

Report type	Intended users	Format	Distribution limitations	Example
SOC 1 (SSAE 16, required after 6/15/11, replaces SAS 70)	<ul style="list-style-type: none"> ➤ Customers financial statement auditors 	<ul style="list-style-type: none"> ➤ Long -form report ➤ Description of controls and systems ➤ Tests performed and results of testing 	<ul style="list-style-type: none"> ➤ Restricted to current customers ➤ Limited distribution to prospective customers 	<ul style="list-style-type: none"> ➤ Payroll processing ➤ Credit card transaction processing
SOC 2	<ul style="list-style-type: none"> ➤ Users seeking assurance over information handling 	<ul style="list-style-type: none"> ➤ “SOC1 look-alike report”: <ul style="list-style-type: none"> ➤ Long -form report ➤ Description of controls /systems ➤ Tests performed &results ➤ Scope relates to “information handling objectives“ (security, availability, processing integrity, confidentiality and/or privacy) ➤ Organization reports controls in place to meet prescribed principles/criteria 	<ul style="list-style-type: none"> ➤ Restricted to users with “sufficient knowledge” ➤ e.g., current <u>and</u> prospective customers, business partners, regulators, employees 	<ul style="list-style-type: none"> ➤ Supply chain information handler reporting on processing integrity ➤ Data center outsourcer reporting on security and availability ➤ Organization’s alignment with ISO 27001 or Cloud Security Alliance framework
SOC 3 (same timing as SOC 2)	<ul style="list-style-type: none"> ➤ Any interested party 	<ul style="list-style-type: none"> ➤ Short-form report ➤ Limited description of controls/systems 	<ul style="list-style-type: none"> ➤ No restrictions ➤ e.g., mass distribution, web-site, current & prospective customers 	<ul style="list-style-type: none"> ➤ Bank reporting on privacy over e-banking application
Agreed-upon procedures	<ul style="list-style-type: none"> ➤ Internal-use ➤ Named business partners 	<ul style="list-style-type: none"> ➤ No description of controls/systems ➤ Report includes only results of specific tests performed and findings 	<ul style="list-style-type: none"> ➤ Restricted to internal and/or named parties 	<ul style="list-style-type: none"> ➤ Compliance with specific controls in vendor contract arrangement

Example of use of SOC 2—Cloud Security Alliance framework

- ▶ Description of the system should address all the questions in the CSA “Consensus Assessments Initiative Questionnaire”
 - ▶ Consider adding an indexing/referencing scheme to make it easier to use
 - ▶ Description should go beyond yes/no to identify how the question is addressed
- ▶ Controls identified by management to address the Trust Services security and availability criteria should be mapped to the CSA “Common Controls Matrix (CCM)” items
 - ▶ Controls may be cross-referenced to CCM controls
 - ▶ Compensating or mitigating controls should be discussed in the description
- ▶ CSA detailed security specifications can be integrated into the description and the contemplated user entity controls

Section 5

▶ Mobile application security

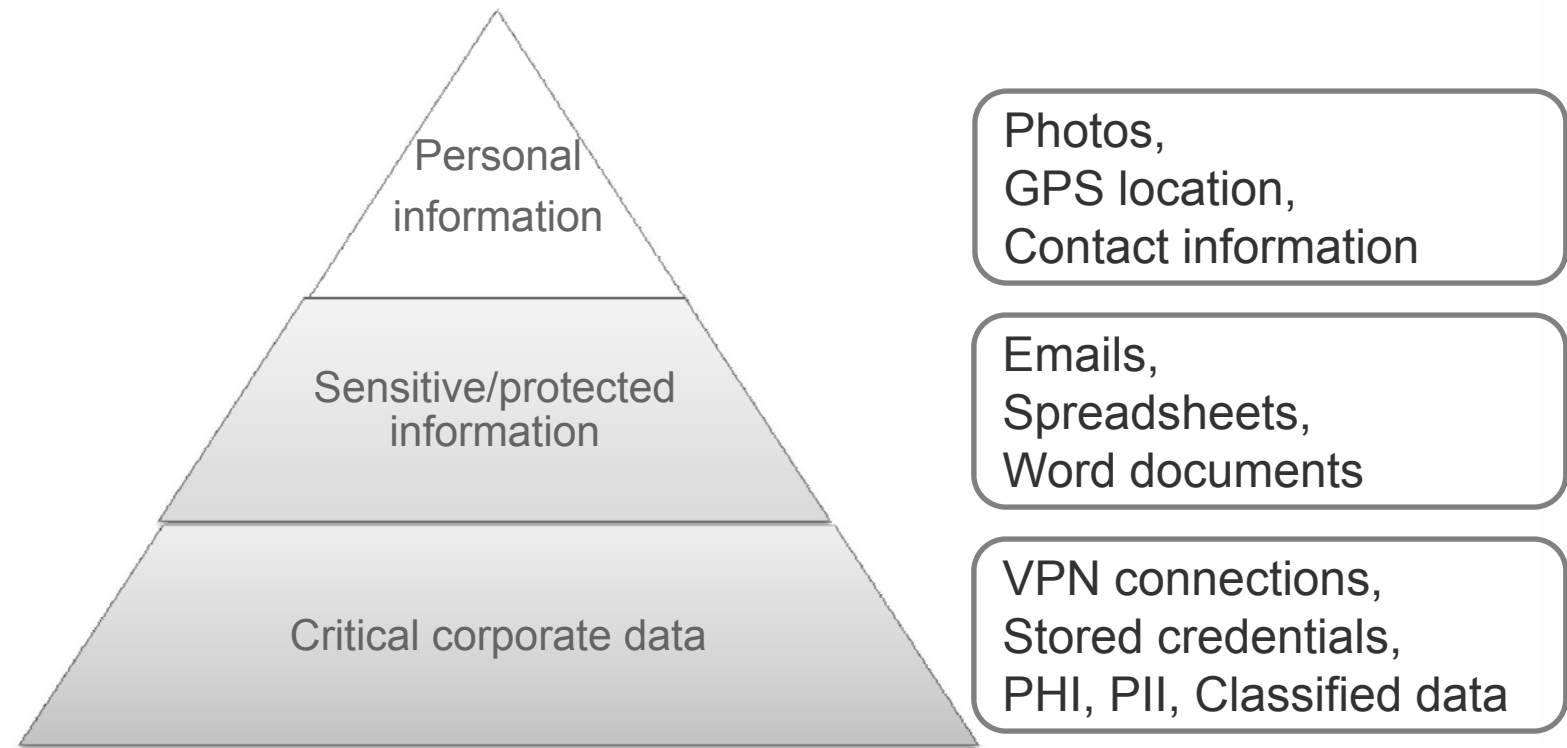
Mobile devices

Fastest growing business technology since PC

- ▶ Enhanced connectivity on the road
 - ▶ Email, calendar, messaging, business applications
- ▶ Greatly increases and decentralizes the systems that need to be secured
- ▶ A high priority initiative for already overloaded IT
- ▶ Multiple disparate platforms to consider and support

Sensitive data on mobile devices

- ▶ Mobile devices may contain sensitive data pertaining to mobile device users and their employers



Mobile device assessments

A few different perspectives

Infrastructure focused

Mobile device configuration review

- ▶ Identifies risks associated with deploying mobile device platforms and supporting infrastructure in an enterprise network.
- ▶ Focuses on the unique implementation for each device platform and policies with which it is configured.

Application focused

Mobile friendly web application assessment

- ▶ Zero knowledge security assessment against web sites designed for mobile devices.
- ▶ External review of supporting infrastructure and servers.

Native mobile application assessment

- ▶ Security assessment of applications installed on mobile devices
- ▶ Provides additional focus on network connections and data handling.
- ▶ Assesses risk of device specific attacks as they pertain to the application

Mobile code grey box assessment

- ▶ Source code assisted security assessment against mobile device applications installed on a device.

Native mobile applications

Risks

- ▶ Contain much richer and interactive environment for the user and significantly more code runs locally to support this
- ▶ Often data is stored locally to be accessed quickly or avoid user reentering
 - ▶ Application credentials
 - ▶ Session information
 - ▶ Payment information
 - ▶ Downloaded documents

Native mobile applications

Risks

- ▶ Platform-specific SDK's require a new set of secure coding skills
 - ▶ Presentation layer security for input fields
 - ▶ Storage of sensitive data securely
 - ▶ Apple's KeyChain
 - ▶ Android's crypto mechanisms
 - ▶ BlackBerry encrypted persistent Object, Key Store
 - ▶ Unmanaged code (memory corruption vulnerabilities)
- ▶ Development pitfalls
 - ▶ Depending on the security of the device
 - ▶ Permitting simpler passwords
 - ▶ Performing security controls on the device instead of the server
 - ▶ Excessive application functionality

Native mobile applications

Security questions to consider

- ▶ What sensitive data is being used by the application?
- ▶ How is data at rest/in transit protected?
- ▶ How is data input/output in the application?
 - ▶ Cell RF, Wi-Fi, Bluetooth, NFC, GPS, etc
- ▶ How is the server secured?
- ▶ What is the proper timeout for authentication?
- ▶ Secure SDLC tollgates
 - ▶ What are the security requirements?
 - ▶ Has a threat model been created?
 - ▶ Have the developers had secure coding training?
 - ▶ Has the application been through a penetration test?

Section 6

▶ Social Media

Several media types fall under the umbrella of Social Media

	Definition and Overview	Examples
Blogs	<ul style="list-style-type: none"> ▶ Blogs are regular entries created by authors to present typically an opinion, an educational piece, or a description of events. Many blogs contain graphics, videos, and links to other articles. ▶ The majority of blogs cater to a specific interest group (i.e. art, technology, sports team, etc). ▶ Currently there are over 112 million blogs registered. ▶ More than 12% of Fortune 500 companies maintain external corporate blogs. ▶ Companies use blogs as a tool to build relationships with customers, or share knowledge internally. 	
Social Networks	<ul style="list-style-type: none"> ▶ Some times called Micro blogging - A type of social media similar to blogs but limited by bit size. ▶ Society is trending away from receiving news and information that is 'pushed' to them. Technology now allows for consumers to pull the content that they desire to consume in a hyper-efficient manner. ▶ Some internet communication is becoming even more bit-sized. ▶ Twitter is a popular social medium that allows messages of only 140 characters. 	
Forums / Message Boards	<ul style="list-style-type: none"> ▶ This type of media consists of communities made up of people with similar interest (i.e. sports team, musician, automobile, geographic area) that allow for people to post their thoughts for others in the community to read and respond to. ▶ Forums / message boards can be used to hold discussions, post inquiries, and share relevant content. They can be viewed as a support group. ▶ A large percentage of forums / message boards are niche communities with high user involvement. 	
Video / Picture	<ul style="list-style-type: none"> ▶ This media type provides a channel for users to share user generated content (UGC) with others including video, pictures, presentations. ▶ Corporations use sites like slideshare.com to aid in perception of company as knowledge leader. ▶ Youtube.com currently hosts over 40% of all videos viewed online. As of January 2009, 6 billion videos were viewed on YouTube. 	

Social Media by the Numbers – Did you know?



facebook

- Over 500 million active users
- More than 20 billion minutes spent on Facebook daily
- More than 60 million status updates each day
- More than 20 million users become fans of brand pages each day
- More than 3 billion photos uploaded monthly
- More than 5 billion pieces of content shared weekly
- Over 70% of Facebook users are outside the United States
- Over 100 million active users access Facebook through mobile devices



twitter

- Over 106 million users
- Over 55 million tweets (messages) sent daily
- 20% of Twitter conversations are about brands, products, services
- Fastest growing social network at 1,382% year over year
- Only 20% of users come via Twitter.com, the rest through mobile devices and 3rd party applications (network effect)
- Approximately 5% of users account for 75% of all activity (influencers)



- Over 350 million people globally read blogs
- Approximately 80 million blog readers in the United States each month
- 4 out of 5 bloggers are writing about brands online
- 12% of bloggers are corporate bloggers
- Bloggers spent 3.5 more hours on the internet than watching TV
- Bloggers are becoming a trusted source of information for consumers (influential blogs)
- 1 out of 3 bloggers have been approached by a brand representative for sponsored posts



Google™

- Over 1 trillion unique web pages in Google's index
- Over 31 billion Google searches monthly
- 684,000,000 visitors to Wikipedia last year
- 14 billion videos watched online monthly by online Americans
- 72% of American consumers are searching online
- 91% of journalists use search engines for research

Social Media is a global phenomenon that continues to shift consumer attention and behavior from traditional media

** Sources: Facebook, Technorati, Twitter, Nielsen, Comscore, Compete*

Social media risks

- ▶ Leaking of sensitive information
- ▶ Social engineering
- ▶ Misuse of social applications
- ▶ Brand and reputation damage

Leaking of sensitive information



[HealthyRandy](#) **LEAKED**: New Pictures And Details Of 's iPad-Killer, The Courier <http://bit.ly/bsSUye> ~ More of a bruiser instead of a 'killer'.

26 minutes ago from web



[ingresosnuevos](#) **Leaked** information hint at future <http://bit.ly/ajXMZh>

33 minutes ago from twitterfeed



[Djbrew07](#) Listening to some of the **leaked** tracks to ushers new album on youtube.

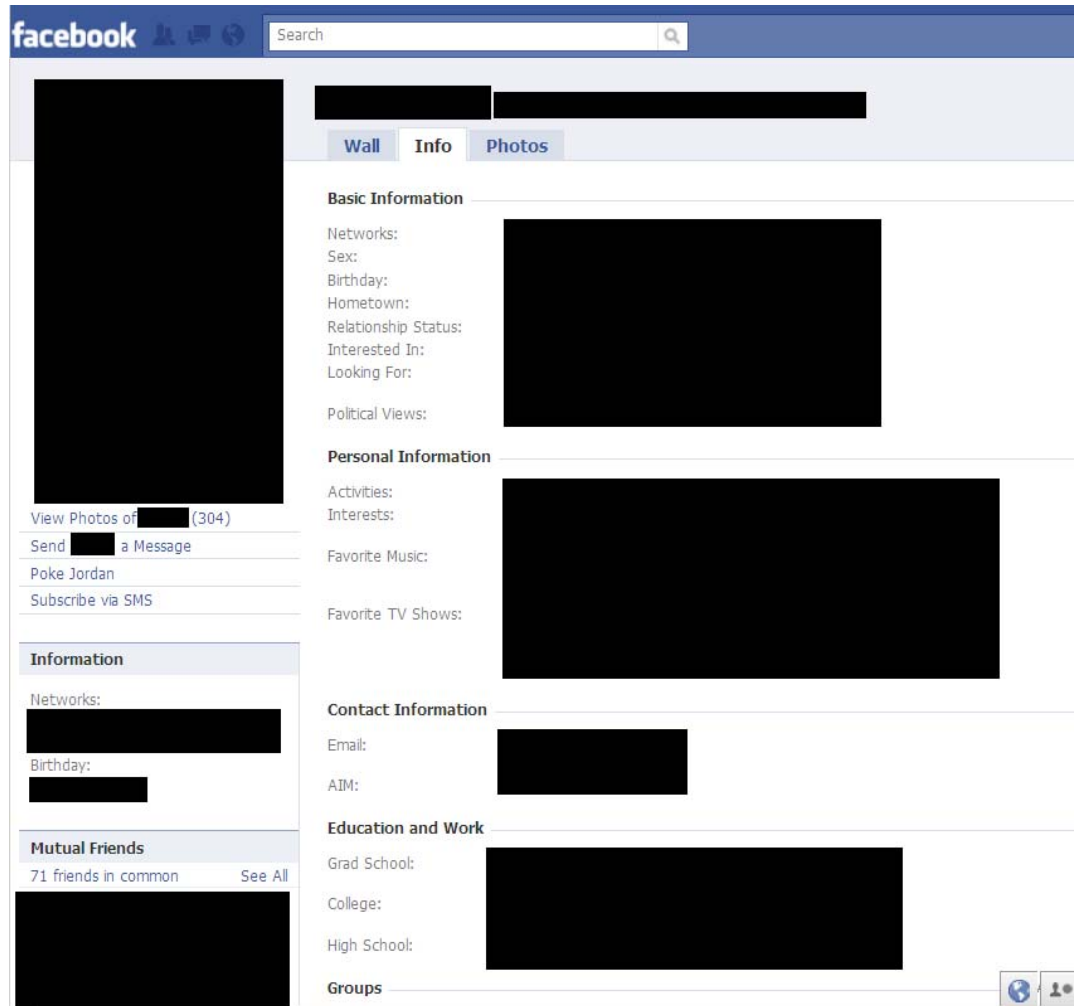
about 3 hours ago from web



[dsawyer](#): Kickass concept art **leaked** - new [REDACTED] project <http://trim.li/nk/9zm> #steampunk

3 days ago from Flock · [Reply](#) · [View Tweet](#)

Leaking of sensitive information



Social engineering



Reset your password

Select an option for resetting your password:

Use my location information and secret answer to verify my identity

Country/Region:

State:

ZIP code:

Question: **which school did i study in**

Secret answer:

Five-character minimum; not case sensitive



Contact Information

Email: [redacted]@hotmail.com

Mobile: [redacted]

Current Address: [redacted]

AIM: [redacted]

Education and Work

High School: [redacted]

Misuse of Social Applications



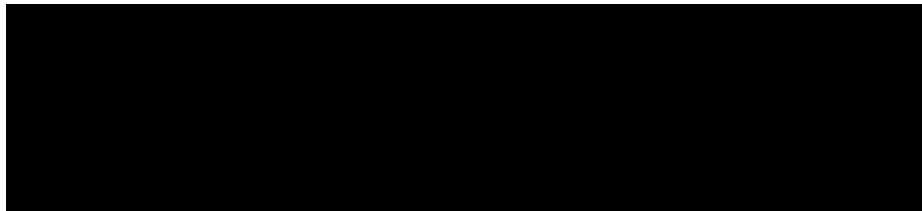
President / CEO at

Area | Telecommunications

Current:

Past:

Keywords:



Connections



83 connections

Brand and reputation damage

Hate my work at [REDACTED]! But its the end!!! holidays J-7!!!!!!!

1:20 PM May 31st from web



many77
Audrey

@MarielMendoza I just took a nap in the theater room at work here on the [REDACTED] lot. Haha. *yawn*

12:52 PM Jul 31st from UberTwitter in reply to MarielMendoza



AustinJose
Austin Jose

Tweeting at work. Anyone want to see a magic trick. Then come to downtown [REDACTED] and visit me at work! I'm a magician btw lol

6:29 PM Jul 31st from TwitterFon



Kris_shreds
Kris matranga

On the PLUS side, 2nd interview with [REDACTED] went well, just waiting on a background check to go through!

6:23 PM Jul 31st from web



TattooedPixie
Pixie

Ok...after almost a week at [REDACTED], work suuuucks.

11:05 AM Jun 8th from txt

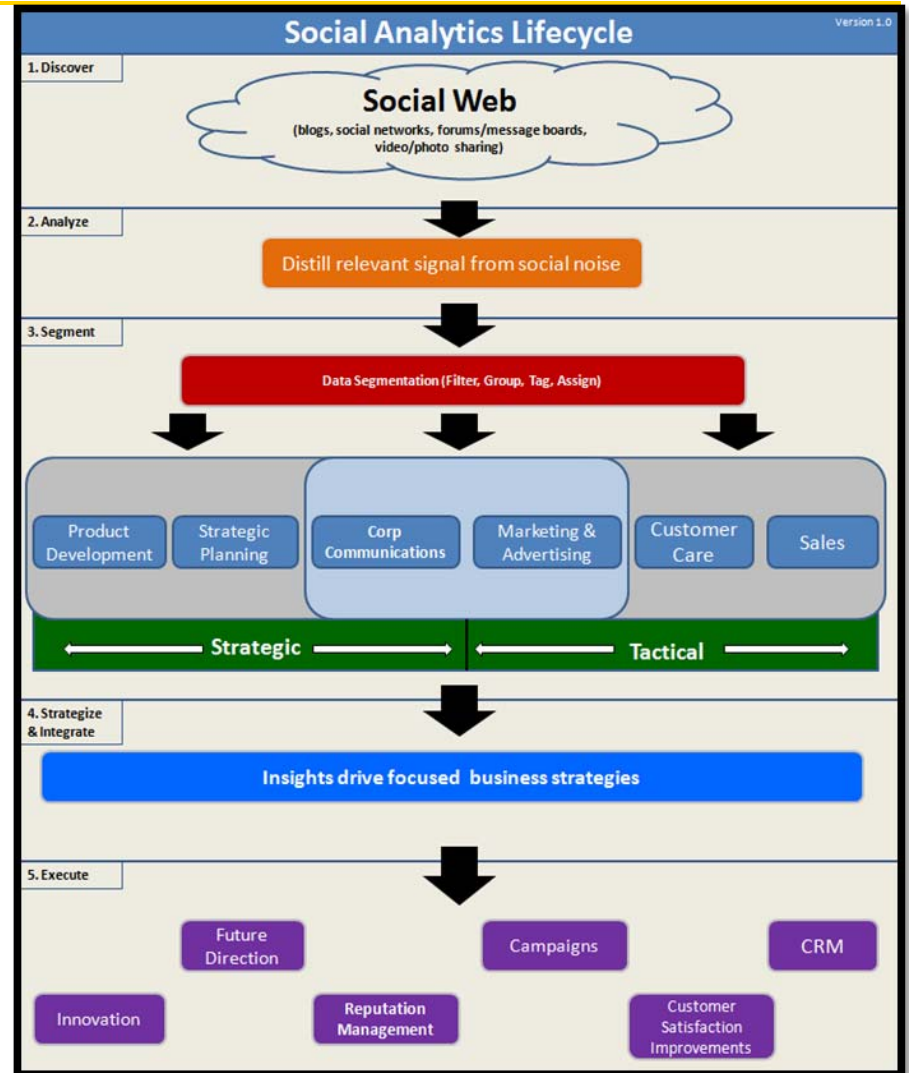


ratmackay
Rat MacKay

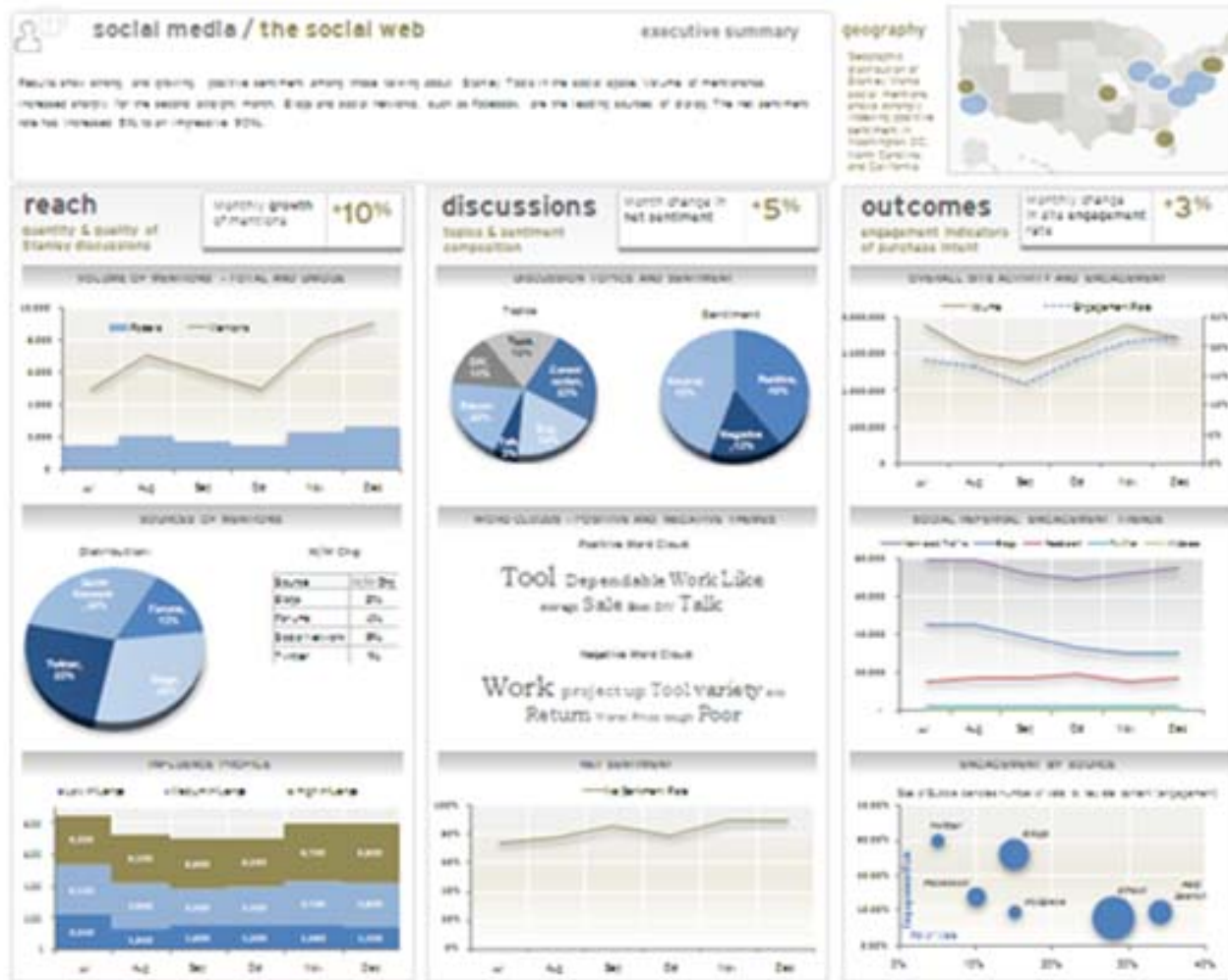
Begin with Monitoring

Monitoring/Listening programs start by discovering relevant social data, synthesizing it into findings, segmenting / prioritizing, and shepherding intelligence internally to key company functional areas.

- 1. Discover** - Harvest relevant social data
- 2. Analyze** - Separate signal from noise
- 3. Segment** - Segment social data by business function and/or defined categories
- 4. Strategize & Integrate** – Make listening outputs a regular input that informs the strategic planning process
- 5. Execute** – Informed action based on insights from strategic listening



Monitoring Dashboards



- Customizable
- Real-time
- Trend watching
- Segmentation
- Workflow

How are other organizations dealing with the risk?

- ▶ Most organizations are just now becoming aware of the risks and are performing risk assessments that outline the pros and cons of social media usage across the company
- ▶ Creating and communicating a social media usage strategy across the company (including objectives and measurement plan)
- ▶ “Knee-jerk” blocking of access to social applications
- ▶ Developing social media usage policies and procedures
- ▶ Providing education & training to employees
- ▶ Developing strategic listening programs to continuously provide monitoring coverage and real-time data/insights (both internal and external)

How is this relevant to internal audit?

- ▶ Identify risks and control matrices to audit upcoming social networking applications
- ▶ Enhance investigations
- ▶ Real-time and trending view of what is important to audit (risk dashboards)

Contact Information

- ▶ Tushar Padhiar – Senior Manager
 - ▶ Phone: 720.931.4566
 - ▶ E-mail: tushar.padhiar@ey.com

- ▶ Eric Scales – Senior Manager
 - ▶ Phone: 312.218.9579
 - ▶ E-mail: eric.scales@ey.com