



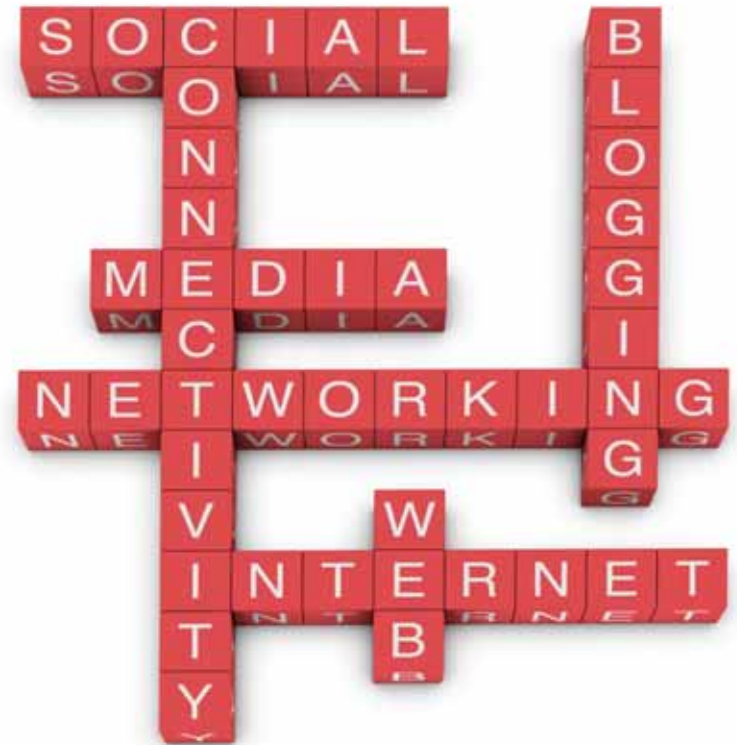
Social Media and How Cyber Criminals Make Use of it to Attack Organizations

**Council of Information Services Directors
Annual Conference**

October 11th, 2011

Michael Wyatt

Deloitte & Touche LLP



Overview of Social Media

Social media

Did you know?

Of the Fortune Global 100, **65%** have active **Twitter** accounts, **54%** have **facebook** fan pages, **50%** have **YouTUBE** video channels and **33%** have corporate **blogs**

– *2010 Burson-Marsteller study*

75% of Internet users worldwide **visit social networks or blogs**; **22%** of the time spent on **Internet usage** is spent on **social media activities**

– *Nielsen Corporation, April 2010*

Facebook has more than **750 Million users**, making it equivalent in population to the **world's third largest country**

-- *Facebook.com, WorldAtlas.com, July 2011*

Social Media Revolution

Social media....it's everywhere!

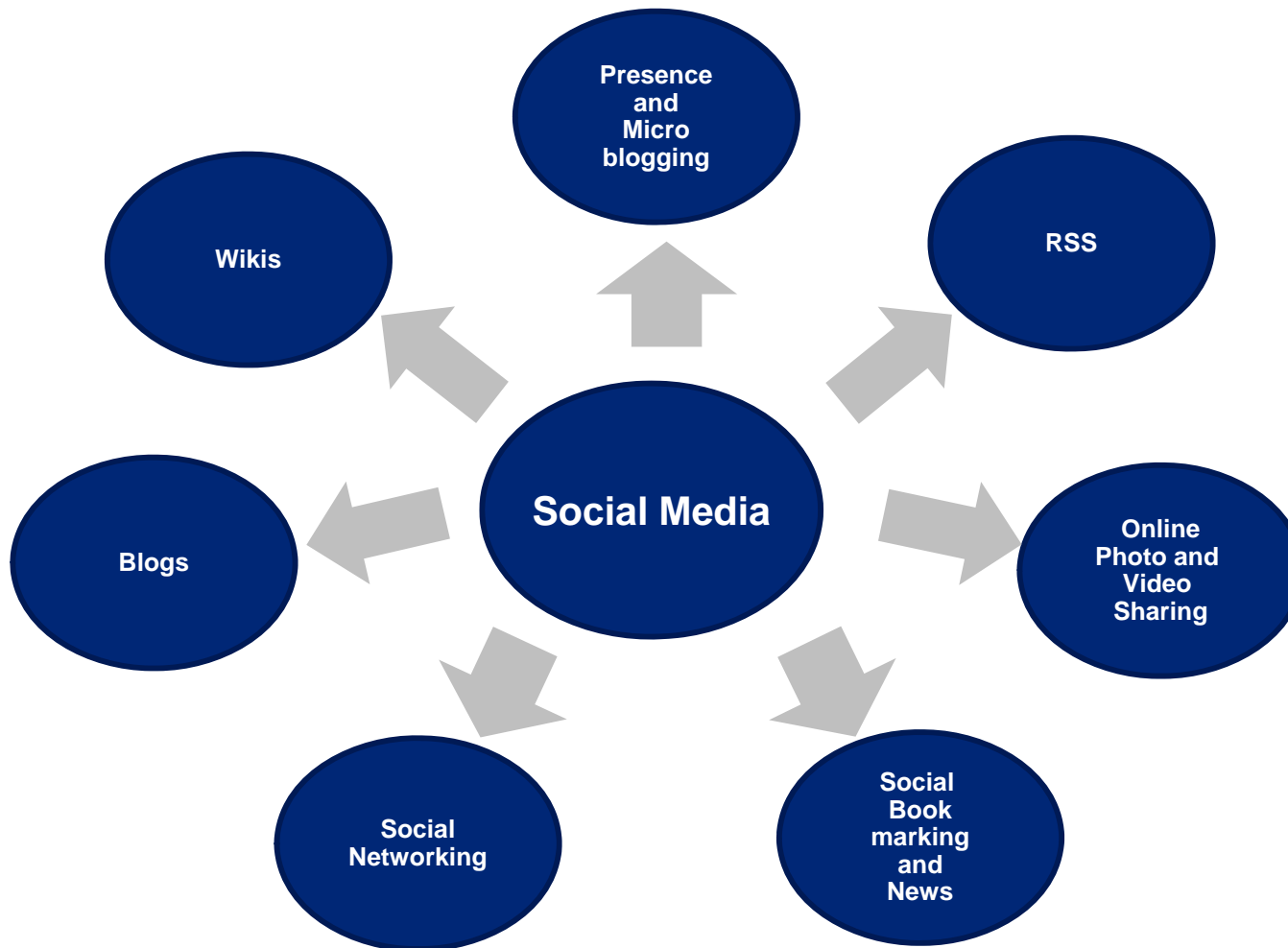


Source: YouTube, *Socialnomics 3* [Video]. <http://www.youtube.com/watch?v=fpMZbT1tx2o>

What is social media?

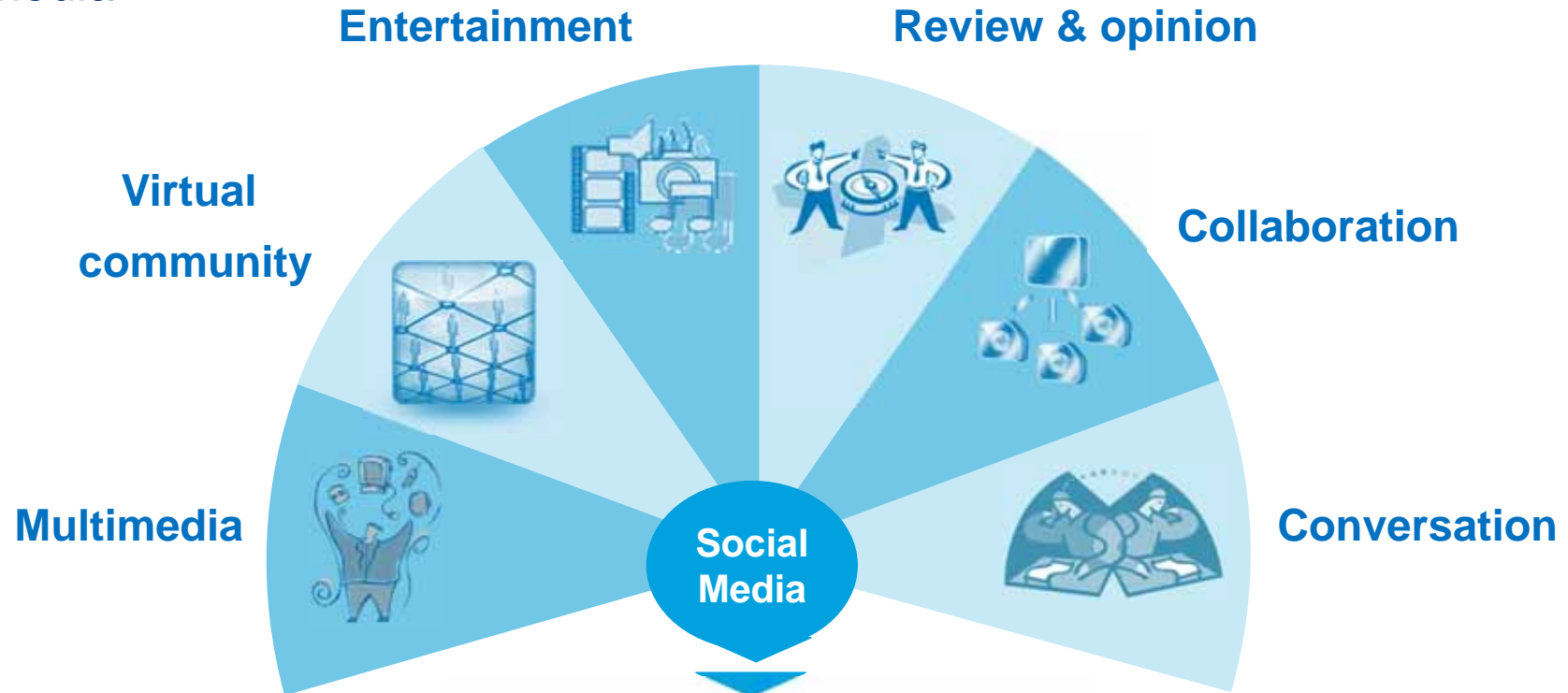
Social media are highly accessible, scalable methods of online communication and social interaction, which allow the creation and exchange of user-generated content

There are 7 main types of social media platforms



Social Media Landscape

Social media is the use of **tools** (e.g., blogs, social media sites) to share content and have conversations, collaborate, review, entertain, build community and share multimedia.



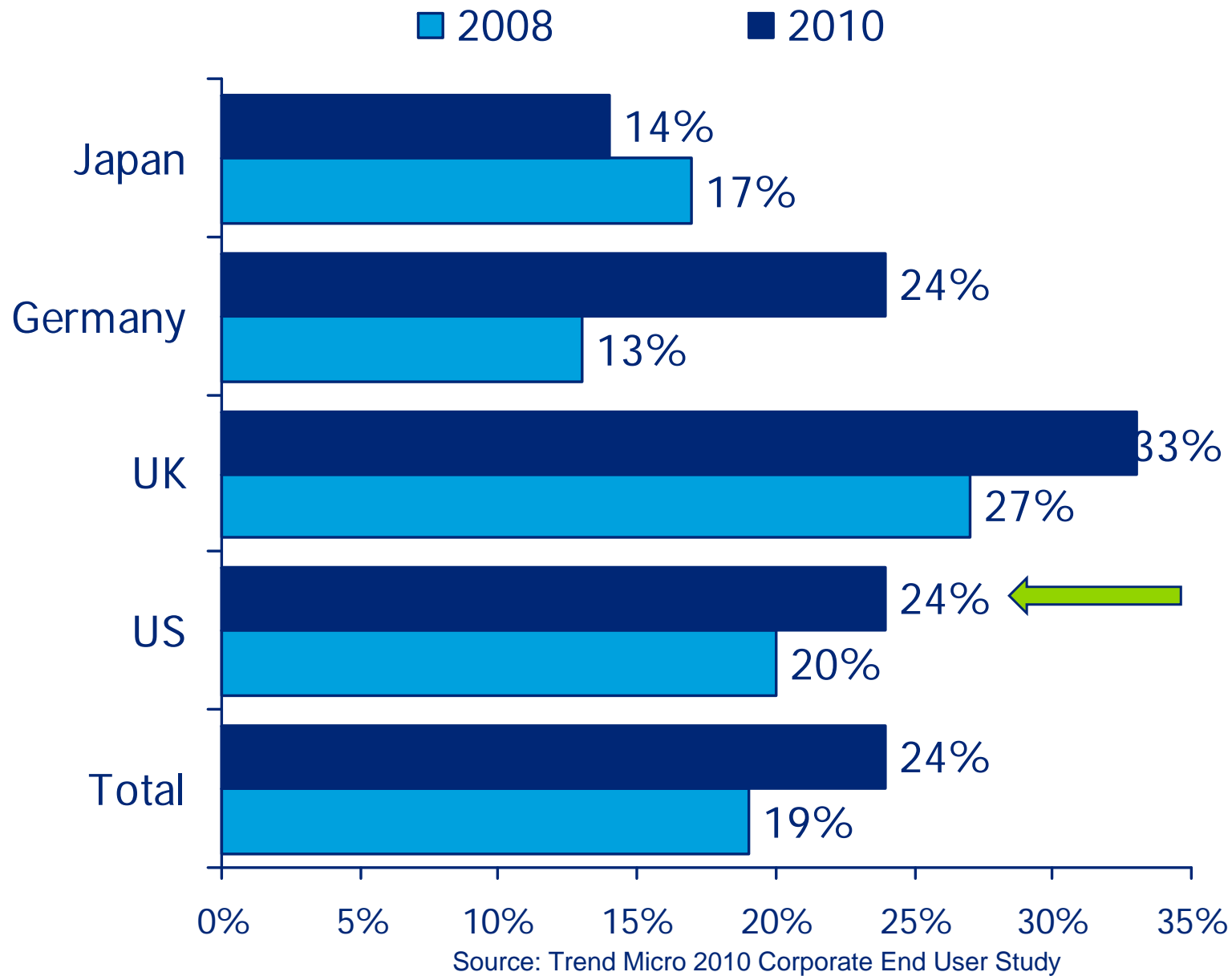
¹The State of the U.S. Mobile Advertising Industry and What Lies Ahead", comScore, June 2011

Social Network Usage

Top 10 Sectors by Share of U.S. Internet Time				
RANK	Category	Share of Time	Share of Time	% Change in
		Jun-10	Jun-09	Share of Time
1	Social Networks	22.70%	15.80%	43%
2	Online Games	10.20%	9.30%	10%
3	E-mail	8.30%	11.50%	-28%
4	Portals	4.40%	5.50%	-19%
5	Instant Messaging	4.00%	4.70%	-15%
6	Videos/Movies**	3.90%	3.50%	12%
7	Search	3.50%	3.40%	1%
8	Software Manufacturers	3.30%	3.30%	0%
9	Multi-category Entertainment	2.80%	3.00%	-7%
10	Classifieds/Auctions	2.70%	2.70%	-2%
	Other*	34.30%	37.30%	-8%

Source: Nielsen NetView – June 2009-June 2010

Social Networking Use While On Organizational LAN



Drivers and Benefits of Social Media

(can't we just shut it down?)

Drivers of Social Networking and Media

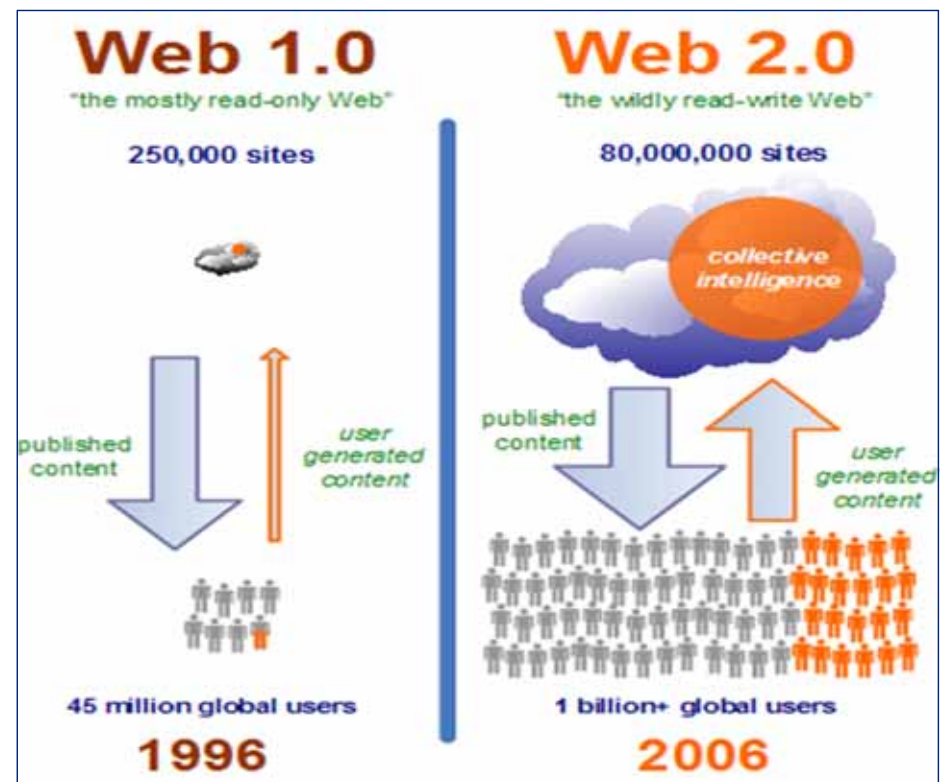
- In the recent years, the end users have taken the control of the Internet transforming its use from a monologue to a dialogue.
- Collaborative problem solving and innovation is leading to higher productivity.
- User's expectation of performance are driven by technology.
- Cultural upbringing of entitlement.

Web 1.0 Inspired by Industrial Age

- Hierarchical (Hierarchy controls and regulates)
- Linear interaction – simple minded
- Organizations innovate
- Organizational segments

Web 2.0 Information Age

- Democratic (Community controls and regulates)
- Network relationship – complex
- Asks customers for products and services
- Customers provide the innovation
- Customers provide the segmentation



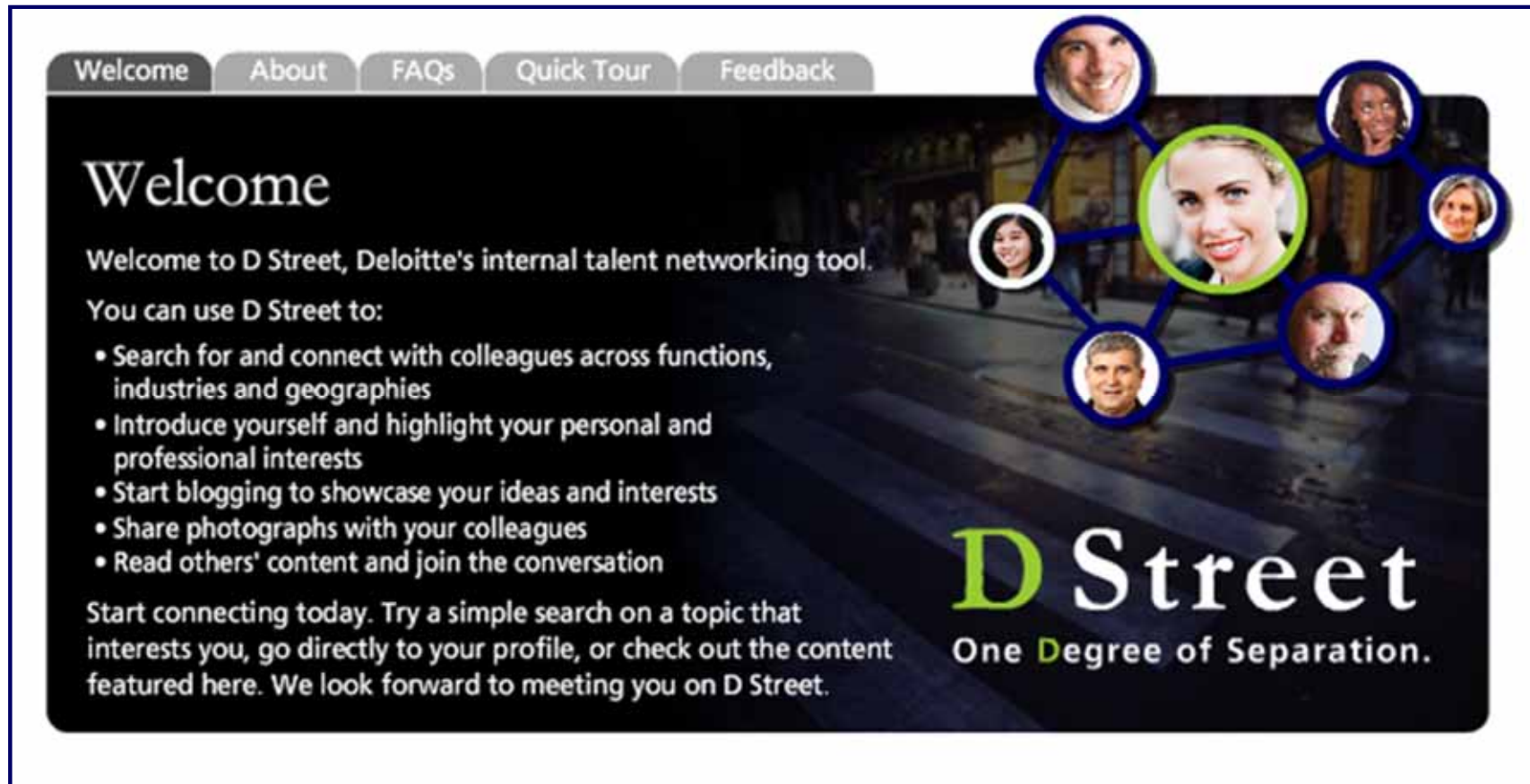
Social Media – For the New Generation

- More than **three-fourths** of workers age 20-29 believe that the “**social**” aspects of work (e.g., connectedness, collaboration) are **very important** to their overall sense of job satisfaction
- However, about **two-thirds** of employees from all generations believe that their organization’s leaders **do not have a clear understanding of the younger generation’s communication preferences and perspectives**



Source: 'Connection' and 'Collaboration' Drive Career Choices for Generation Y Workers, SelectMinds Study Finds. Business Wire, Feb 2007.

Human resources example – D Street



The image shows a screenshot of the D Street website. At the top, there is a navigation bar with buttons for 'Welcome', 'About', 'FAQs', 'Quick Tour', and 'Feedback'. The main content area has a dark background with a network diagram of people's faces connected by lines. The text on the page reads:

Welcome

Welcome to D Street, Deloitte's internal talent networking tool.

You can use D Street to:

- Search for and connect with colleagues across functions, industries and geographies
- Introduce yourself and highlight your personal and professional interests
- Start blogging to showcase your ideas and interests
- Share photographs with your colleagues
- Read others' content and join the conversation

Start connecting today. Try a simple search on a topic that interests you, go directly to your profile, or check out the content featured here. We look forward to meeting you on D Street.

D Street

One Degree of Separation.

11,325 professionals have social profiles, with hundreds more joining every week

Discussion Point

- Does your organization have an official policy for social media use?
- How many organizations block access to social media sites?

*The information discussed during this presentation will not be shared outside the meeting attendees or for any other purposes.

Social Media Risks

Social Media – Blast from the Past

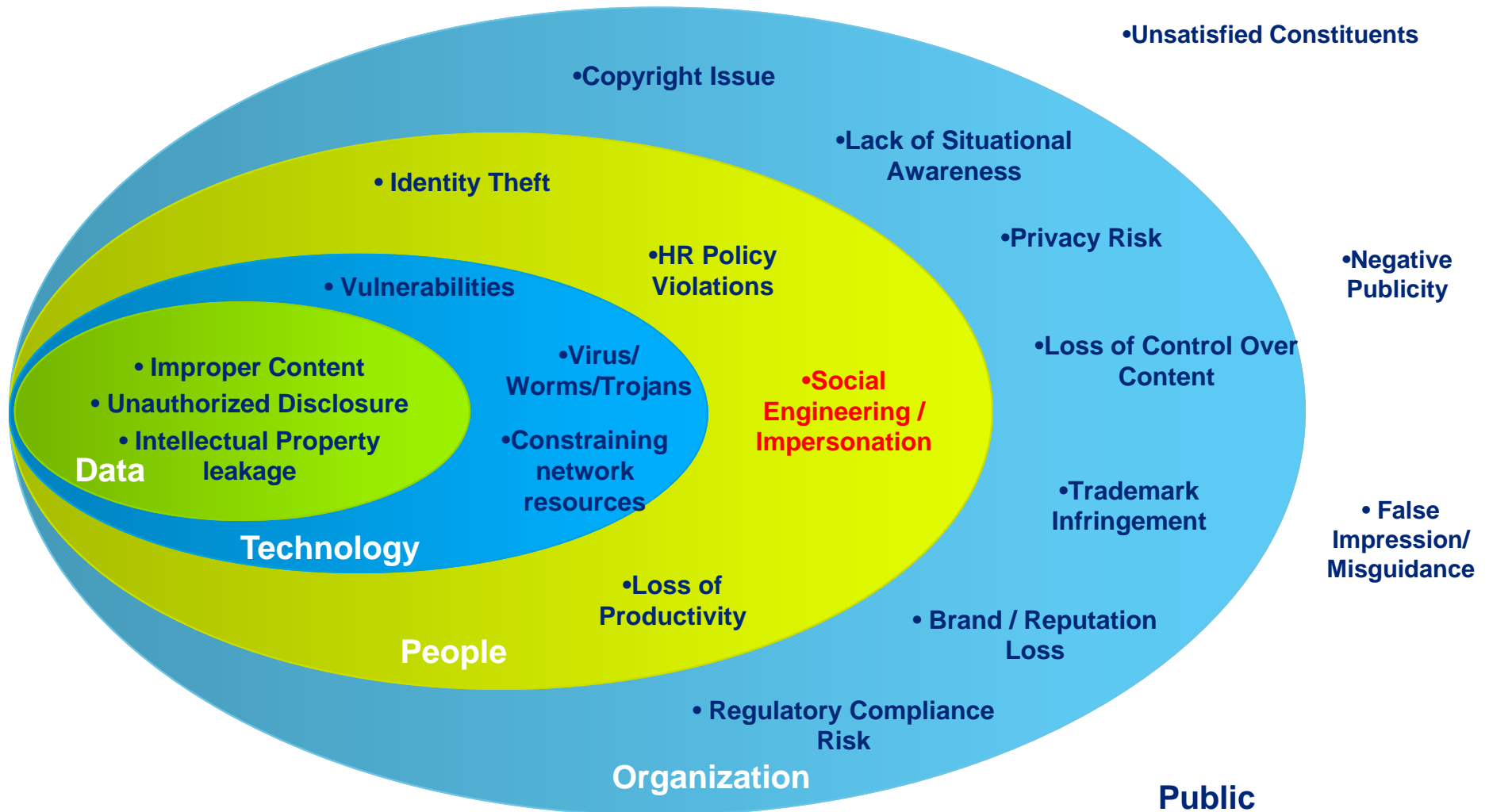
Usage of social media may have been a blessing for some but there have been incidents involving social media which may be thought provoking. Some of these incidents are listed below:

- Employees at a Medical Center in California posted patient information on Facebook.
- A Wisconsin employee was fired for a post she made on her Facebook page claiming that she was addicted to alcohol and various prescription and illegal drugs, although the employee claimed that her comments were made in jest.
- A hospital employee in Hawaii with access to patients' medical records illegally accessed another person's records and posted on MySpace that the individual had HIV.
- An employee used Twitter to post insulting comments about the city government shortly before presenting to the worldwide communications group at a local Company. An employee of the local Company discovered the tweet, responded to the tweeter, and then copied the Company's management.



Social Media – High-level Threat Landscape

The advent of Social Media into the corporate environment brings along multiple risk to the Data, Technology, People, and Organization.



Social Media – Threat Landscape, con't

In addition to the benefits of social media, there are a number of techniques and threat vectors that can lead to a number of social networking exploits.

Techniques

- Use social networking sites to profile and enumerate users
- Taking information learned and using it for social engineering schemes such as targeted phishing messages
- Getting unsuspecting users to install 3rd party fraudulent applications which provide access to entire user profile
- Emails with profile pictures from friends are being used to get users to click on links
- Using short URLs to obfuscate malicious links bit.ly
- Using compromised accounts of friends
- Celebrity impersonation

Threat Vectors

- Blogging
- Chat
- Email
- File sharing
- Document meta data
- Open APIs
- Third party applications
- Third party services
- Video
- Voice chat

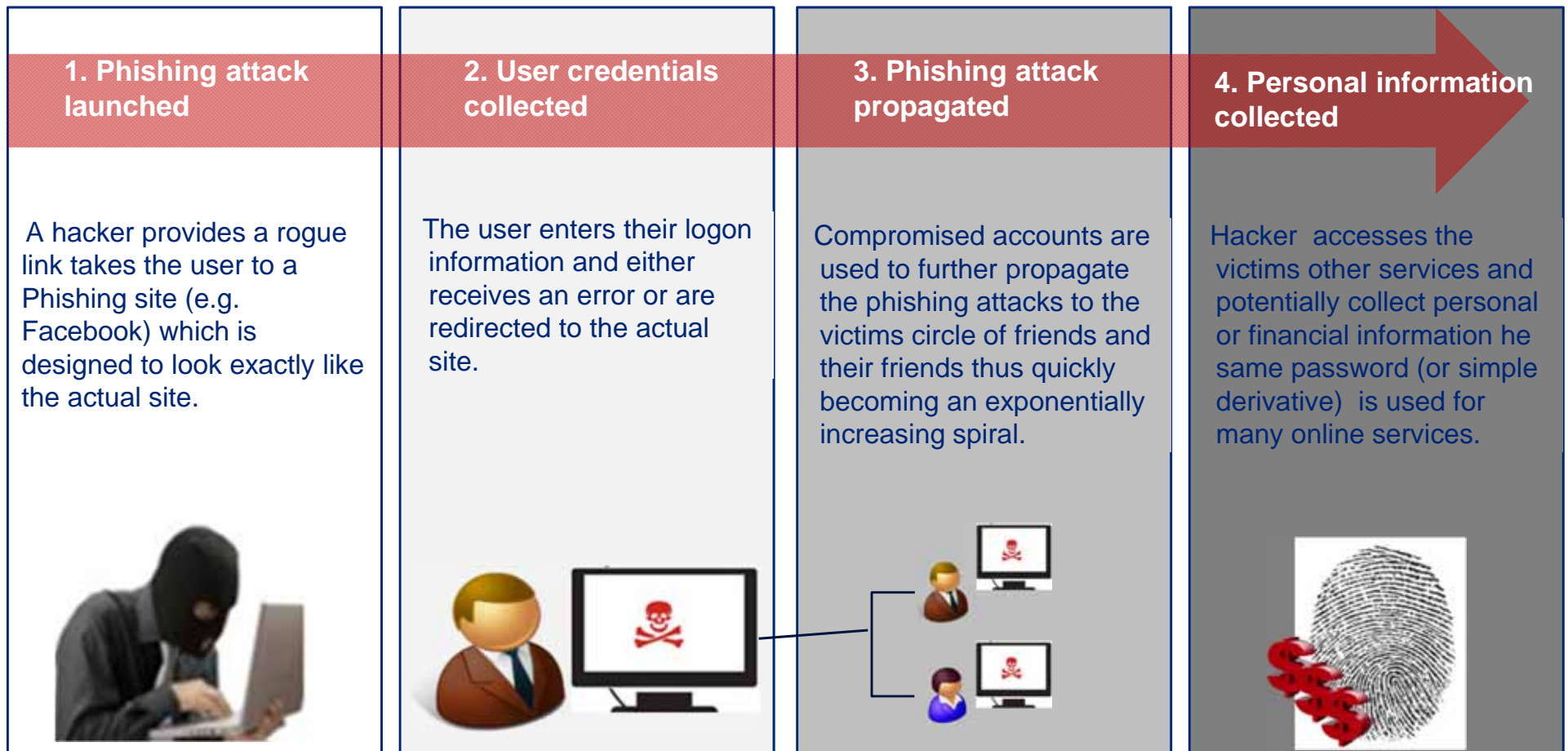
Social Networking Exploits

- Social Networking account hi-Jacking
- Social Networking brand hi-Jacking
- Black hat search engine optimization
- Botnet command and control
- Distributed Denial of Service attacks
- Hack for Hire Schemes
- Man in the Middle Attacks
- Click-jacking / Cookie Stuffing
- Full browser control by 3rd party applications
- Twitter spam
- Follower spam-spam links on profile pictures leading to malware
- Malicious banner ads
- Malicious background images
- Spear Phishing

Social Media Attacks - Phishing

There can be high costs associated with either a breach or leakage of information depending on the industry in which the breach occurs. In 2010, over 43% of Social Media users reported being targeted by Phishing attacks via the Sites. This is double the 2009 number and is projected to significantly increase in 2011.

[MessageLabs Intelligence: 2010 Annual Security Report](#)



Social Media Attacks - Malware

Installation of Malware, Trojans and other malicious software is by far the most dangerous form of attack.

Facts

- In 2010, there were 95,000 new unique malicious programs very day – double the rate of 2009, almost one every 0.9 seconds.

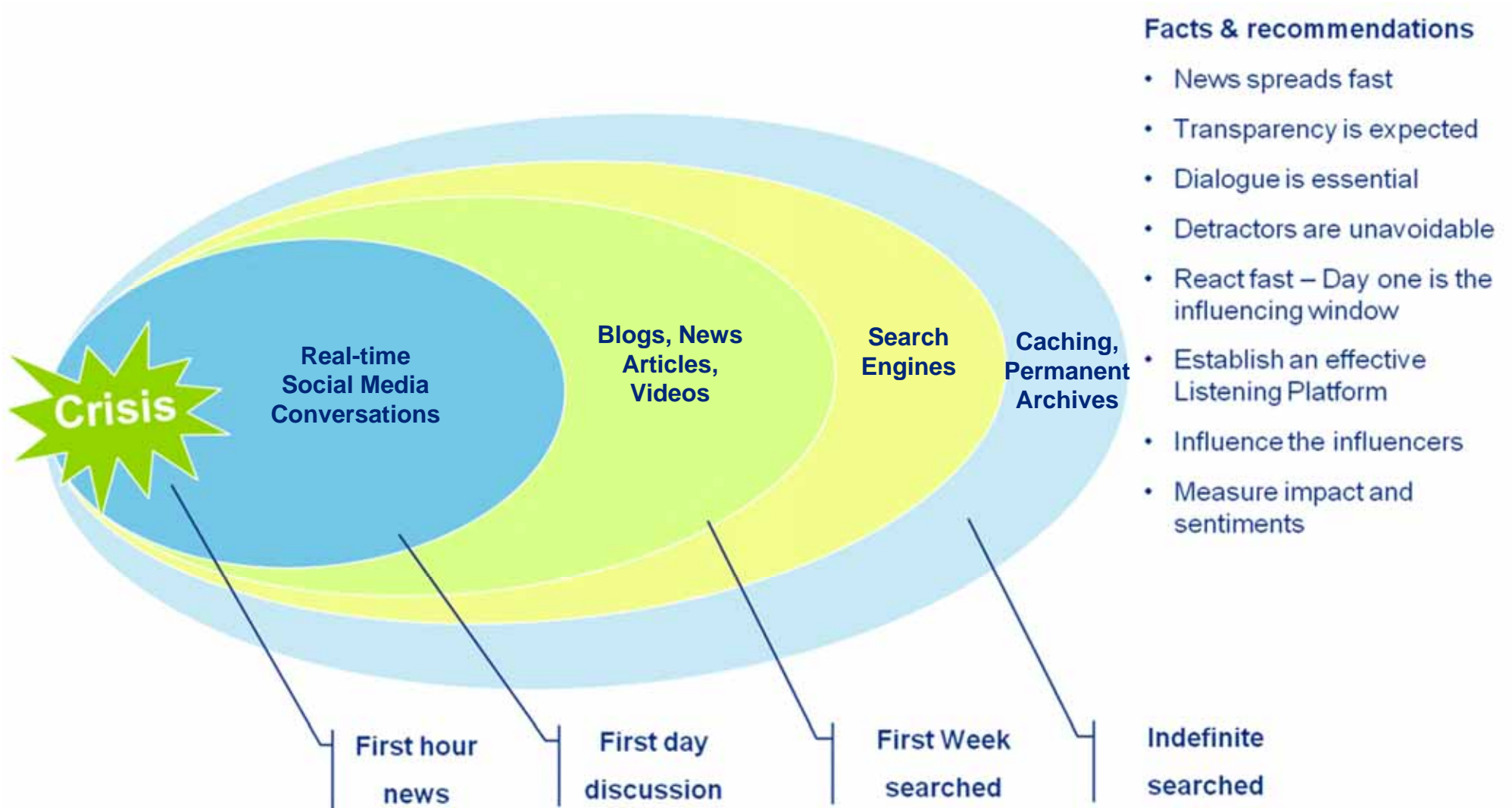
[Sophos 2011 Security Threat Report](#)

- Similarly in 2010 over 6000 new vulnerabilities were reported. This includes a 43 percent increase in mobile vulnerabilities between 2009 and 2010 (from 115 to 163)

Malware in action

- Malware typically exploits vulnerabilities in the underlying operating system (such as Windows) or in the common applications (such as Acrobat Reader or Microsoft Word).
- These malicious programs range from fake anti-virus programs (that make a computer unusable by disabling several processes and popping up fake virus alerts – until you buy their “anti-virus”) to key loggers to very sophisticated code that gives the attackers control of the compromised computers.
- Rustock, one of the biggest botnets in 2010 had at its height over one million bots under its control. Similarly other botnets also had hundreds of thousands machines under their control.

Detour: Brand and Crisis Management



Discussion Point

- Do you think your organization is currently prepared to handle social media risks?
- What areas are currently well covered? What areas are not?
- What tools do you have in place to help?

Strategies

Public Sector Response

- The US Department of Defense has provided formal guidance on the use of Web 2.0 tools
- The US State Department's official policy, Using Social Media, requires a site sponsor to be the record keeper for content that must be preserved long term
- Federal Energy Regulatory Commission (FERC) Order No. 717 requires monitoring and archiving of communications between the marketing and transmission operations of vertically integrated electricity and natural gas companies.
- The Environmental Protection Agency has published Interim Guidance for EPA Employees who are Representing EPA Online Using Social Media

Current Observations - Social Media Controls

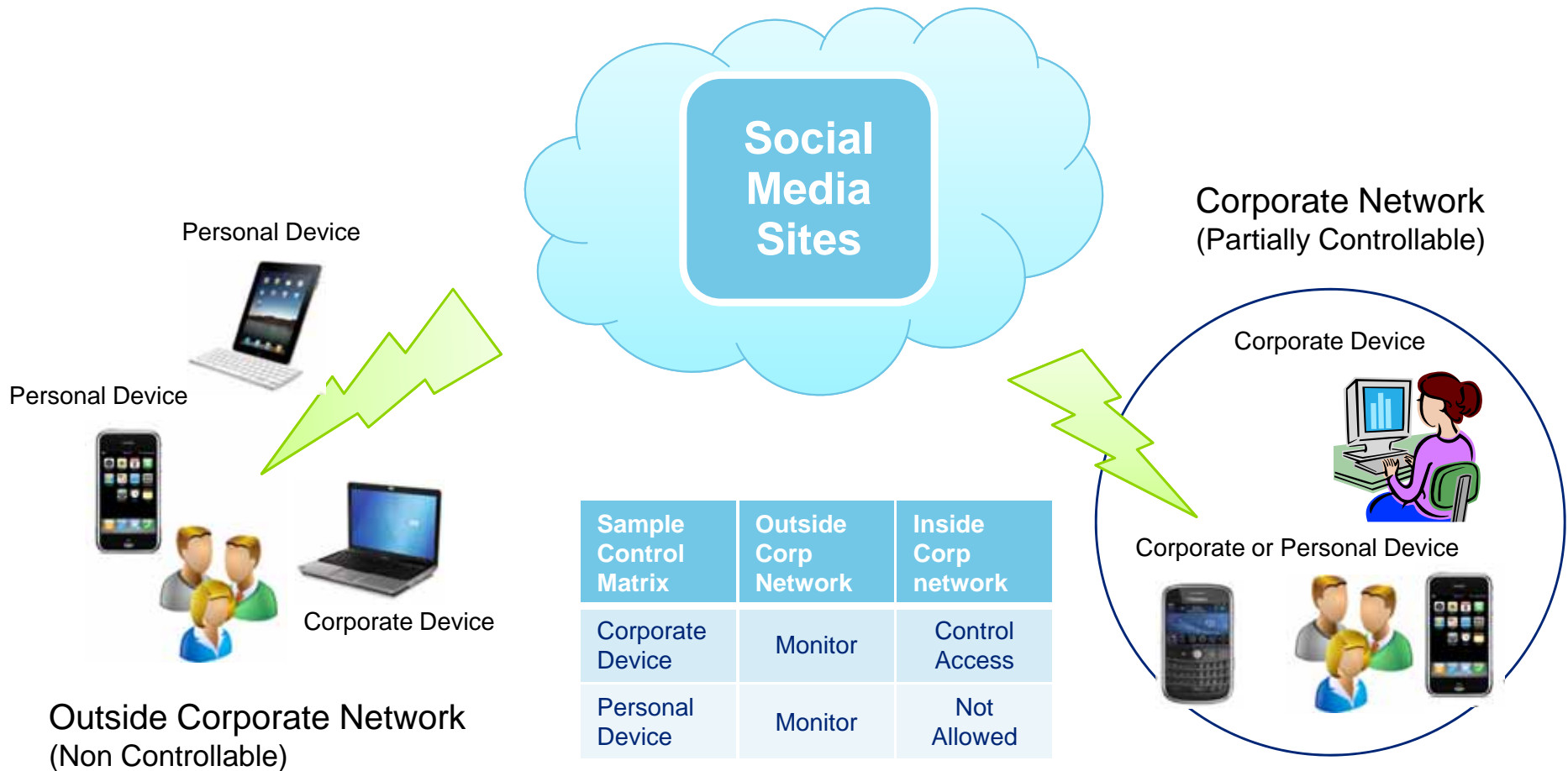
The control of social media in the corporate environment is lack of consistent practice. Based on our observations, organizations' control approach generally falls into the following categories:

- **No Policy:** organizations have not formed a direction on how to use and/or control social media platforms. Employees are able to access social media sites using both corporate-issued or personal devices
- **Block*:** organizations take a risk-averse philosophy and block employees' access to social media sites when users reside within the corporate network
- **Limited Access*:** organizations limit access to social media sites to certain departments or business areas only (e.g., marketing, corporate communications, human resources); most of usage of social media is for promoting corporate brand, sharing general/public business information, or for recruiting purposes; usually a small number of users are allowed to access social media sites
- **Controlled Access:** organizations wants to adopt social media as a productivity improvement tool to further client collaborations and communications, strengthen customer relationships, and integrate social media as part of business transaction platforms; this approach requires organizations have clear policies and guidance, educate and train employees, as well as implement technologies to meet security, privacy, and record retention requirements.

** It should be noted that blocking and limiting users' access to social media sites only work within the corporate network environment. There are no effective ways of restricting users' access when they use public Wi-Fi, hotel network, home network, cellular network, etc.*

Current Observations – Technology Usage

The adoption of mobile devices, corporate initiatives on Bring-Your-Own (BYO) devices, and the increasing blurry lines between corporate and non-corporate network boundary have led to significant challenges in enforcing technical controls to policy social media site access or usage.



There is no single technology that can control the access and usage of social media. Organizations need to establish a control matrix based on use scenarios and set clear policy and guidance.

Social Media Risk Management Principles

From the legal and regulatory requirements, we observe that SEC, FINRA and various other institutions has made it obligatory for organizations to implement risk management practices in Social Media.

Policies and Education



- Defines the usage and participation policies in Social Media tools
- Educate employees with these policies and/or guidance

Monitoring and Listening



- Supervise the release of certain business content
- Monitor communications with business entities, partners, public, and clients

Controlling and Supervising



- Implement controls to restrict posting and downloading
- Establish accountability of individual user access
- Authorize access based on business need & risk consideration

Archiving and Retention



- Retain and preserve records in a non-accessible manner
- Maintain archives in an exclusively non-rewritable, non-erasable format.
- Keep a duplicate copy of the original in a secure fashion

ISACA Business Model for Information Security (BMIS) and Social Media

1. Strategy and Governance

- Has a risk assessment been conducted to map the risks to the enterprise presented by the use of social media?
- Is there an established policy (and supporting standards) that addresses social media use?
- Do the policies address all aspects of social media use in the workplace—both business and personal?

2. People

- Has effective training been conducted for all users?
- Do users (and customers) receive regular awareness communications regarding policies and risks?

Source: ISACA, *Social Media: Business Benefits and Security, Governance and Assurance Perspectives [Whitepaper]*.

ISACA Business Model for Information Security (BMIS) and Social Media (continued)

3. Processes

- Have business processes that utilize social media been reviewed to ensure that they are aligned with policies and standards of the enterprise?
- Are change controls in place to ensure that changes or additions to processes that leverage social media are aligned with the policy prior to implementation?

4. Technology

- Does IT have a strategy and the supporting capabilities to manage technical risks presented by social media?
- Do technical controls and processes adequately support social media policies and standards?
- Does the enterprise have an established process to address the risk of unauthorized/fraudulent use of its brand on social media sites or other disparaging postings that could have a negative impact on the enterprise?

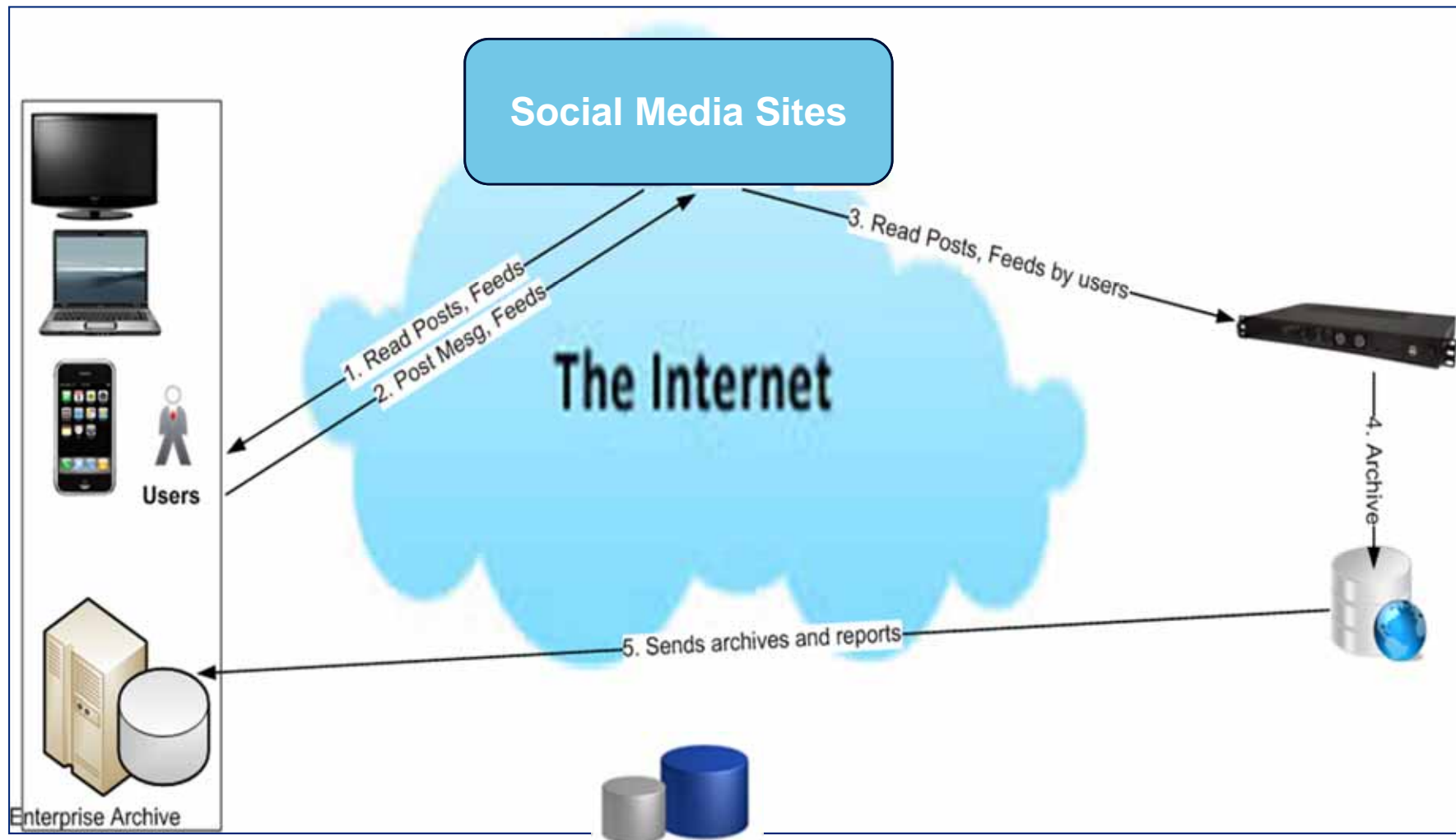
Source: ISACA, *Social Media: Business Benefits and Security, Governance and Assurance Perspectives* [Whitepaper].

Social Media Strategy Recommendations

- **Mobile and Social Media Profiling**
 - Identify current and future organizational needs of using mobile devices and social media sites
 - Confirm and inventory the current technologies (agency / division devices, personal devices, security and archive solutions)
 - Develop a mobile and social medial control matrix to clearly identify current controls (e.g., see Appendix for a sample)
- **Risk Analysis**
 - Confirm regulatory requirements
 - Compare current controls (from the control matrix) to requirements
 - Identify control gaps, internal/external threats, and risks (considering impact and probability)
 - Develop risk mitigation strategy (e.g., risk avoidance, risk transfer, risk remediation)
- **Control Strategy and Roadmap**
 - Select control options (Policies vs. Technologies) to support the mitigation strategy
 - Evaluate future technology and vendor products if needed
 - Develop an implementation roadmap (e.g., estimate on resources, investment, and timeline)
 - Establish a social media governance team

Social Media - Technology Solutions Illustration (cont'd)

Organizations may consider implementing a security solution/ tool that is hosted internally or externally which allow them to archive and retain an inaccessible and indestructible copy of the communication. These records may be subject to reviews and/or audits at a later period of time as and when required.



Additional Considerations

Cyber Threat Profile Analysis

Perform a study on what organization specific foot printing information is available on the Internet, and how it might be used to produce an exploit that targets the organization's IT or Industrial Systems.

Intranet Cyber Compromise Diagnostic

Security event logs and infrastructure logs are analyzed to look for evidence of internal machines that may have been compromised and are attempting to communicate with miscreant controlled devices on the Internet.

Suspicious Program Diagnostics

Use available industry hash data sets and cyber intelligence to match against a generated inventory of system files endeavoring to identify hidden exploits. Perform digital forensic analysis on suspect computers including examining system memory.

Anti-Phishing Capability Diagnostic

Assess organizations' anti-phishing program in order to help identify gaps and improvement opportunities. It includes looking at recent phishing incidents, intelligence services, and the organization's incident handling procedures.

Social Media Impact Survey

A policy assessment is performed to assess how social media is being used within the organization.

Questions?

References

- Sophos Security Threat Report – 2011 by Graham Cluley
- Cisco 2010 Annual Security Report
- KOOBFACE – Inside a Crimeware Network by Nart Villeneuve of the Information War Monitor
- Symantec Internet Security Threat Report – Volume 16, April 2011



Contact info

Mike Wyatt

Security & Privacy Leader

State Government

Deloitte & Touche LLP

+1 512 771 8062

miwyatt@deloitte.com

Rob Thrash

Senior Strategic Relationship

Manager

Deloitte Services LP

+1 416-601-5938

rthrash@deloitte.com



This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this presentation.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.