



Addressing the security challenges of two emerging technologies: Mobility and Web2.0

Public Sector Information Security
Conference - 23 July 09, Sydney



Mobility & Access to Information: Agenda

- Business Drivers for Mobility & Web 2.0 Services
- Intro to Web 2.0 & Mobility
- Corporate Response - Permit or Deny
- Current trends & relevance
- Mobility Security Issues
- Web Application Security Issues
- Conclusion

We are going to be talking a lot about current statistics

So I thought I would put this disclaimer in



DISCLAIMER

"42.7 percent of all statistics are made up on the spot."

--The Hon. W. Richard Walton, Sr.

.... But I believe I am using credible sources and it is all referenced





Mobility & Access to Information: Agenda

- Business Drivers for Mobility & Web 2.0 Services
- Intro to Web 2.0 & Mobility
- Corporate Response – Permit or Deny
- Current trends & relevance
- Mobility Security Issues
- Web Application Security Issues
- Conclusion



Business needs for mobility and social networking/collaboration tools:

- Efficient access to information from remote locations
- Provide practical and reliable access to shared information regardless of geographical location and/or time zone
- A desire to leverage contacts and content in more effective ways
- Flexible work location options help retain skilled staff
- Increase productivity levels in competitive markets
- Reduce operational costs- compelling ROI

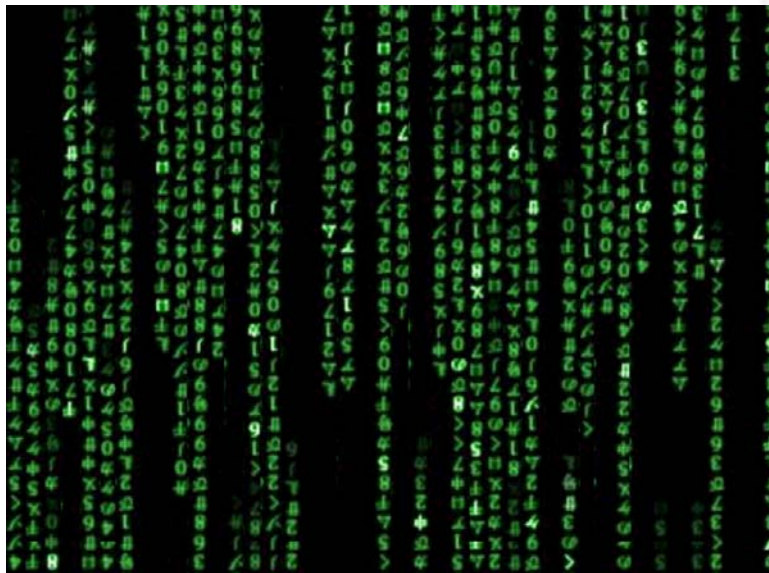


People and Information

It's all about
giving



access to



securely!





Mobility & Access to Information: Agenda

- Market Drivers for Mobility & Web 2.0 Services
- **Intro to Web 2.0 & Mobility**
- Corporate Response - Permit or Deny
- Current trends & relevance
- Mobility Security Issues
- Web Application Security Issues
- Conclusion



What is Web 2.0?

Web 2.0 refers to today's "second generation" of Web technologies

- includes AJAX, RSS feeds, online forums, and mashups.

In general Web 2.0 covers broader development trends:

- Rich Internet Applications (RIA): Feature rich web sites; mimic thick client applications.
- Collaboration and Participation: Generating and sharing content in real time; wikis, extranets, blogs, social networking sites, online forums.
- Syndication: RSS or Atom feeds and mashups. Broadcasting of data.



What is Web 2.0?

"Web 2.0" refers to the second generation of web development and web design. It is characterized as facilitating communication, information sharing, interoperability, user-centered design and collaboration on the World Wide Web. It has led to the development and evolution of web-based communities, hosted services, and web applications. Examples include social-networking sites, video-sharing sites, wikis, blogs, mashups and folksonomies.

[Ref: Wikipedia]

In contrast to the static nature of Web 1.0, Web 2.0 systems rely heavily upon user generated content. In fact, Web 2.0 has been described as the "participatory Web."

[Ref: Secure Enterprise 2.0 Forum, Top Web 2.0 Security Threats, 2009]



Look familiar?

Social Networks



Instant Messaging



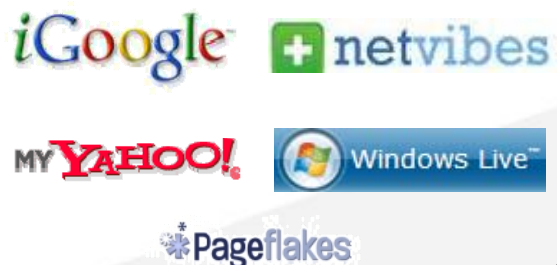
RSS



Tagging



Personalised Home Pages



Widgets



[Source: Worklight]



Thousands already and growing daily



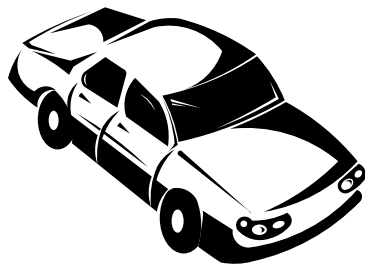
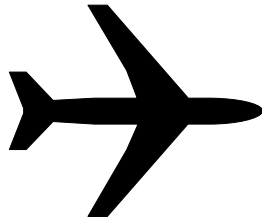
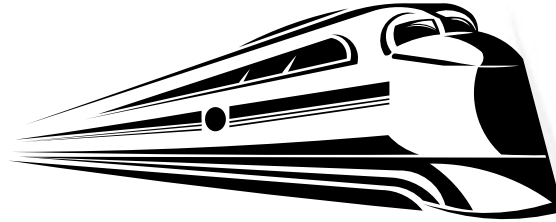
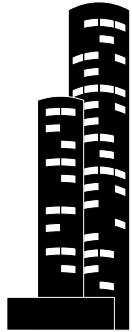


Show me the access!

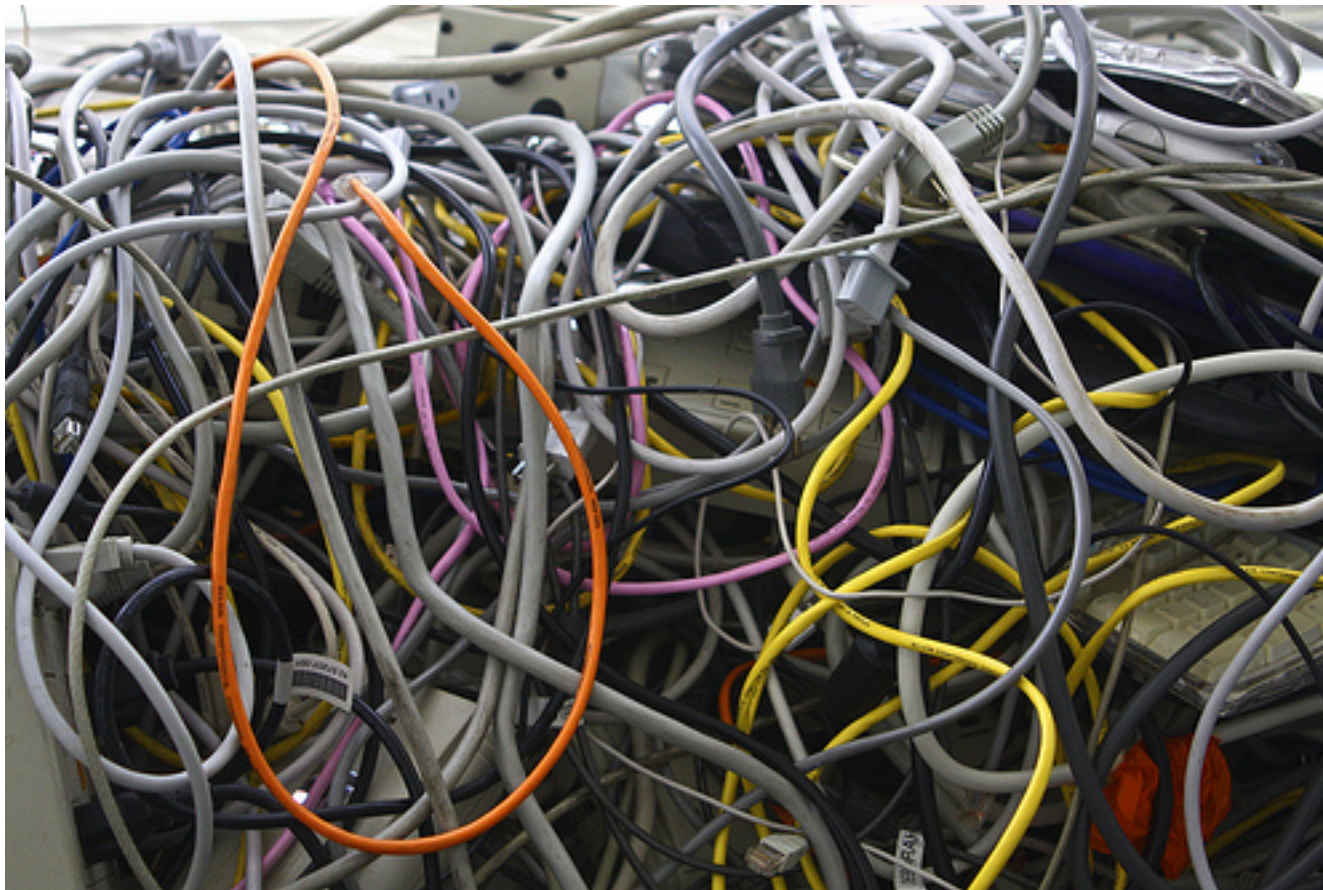
So you provided the platform to share the information, now how do I access it, use it and store it?



Access required from everywhere



Forget about the cables



We need mobility, availability & storage



“96% of the time people have their cell phones
within 1 meter of them”

[Ref Tony Saigh, business development manager for mobile at Skype
<http://www.cnet.com.au/skype-s-mobile-dreams-339285053.htm>]

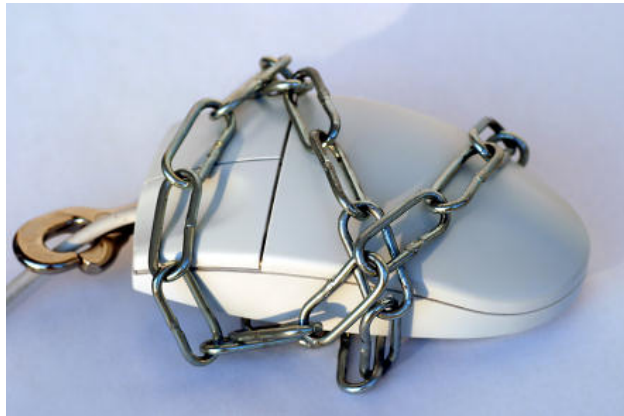


Mobility & Access to Information: Agenda

- Market Drivers for Mobility & Web 2.0 Services
- Intro to Web 2.0 & Mobility
- **Corporate Response - Permit or Deny**
- Current trends & relevance
- Web Application Security Issues
- Mobility Security Issues
- Conclusion

The corporate response

The usual (corporate) response is a mixture between



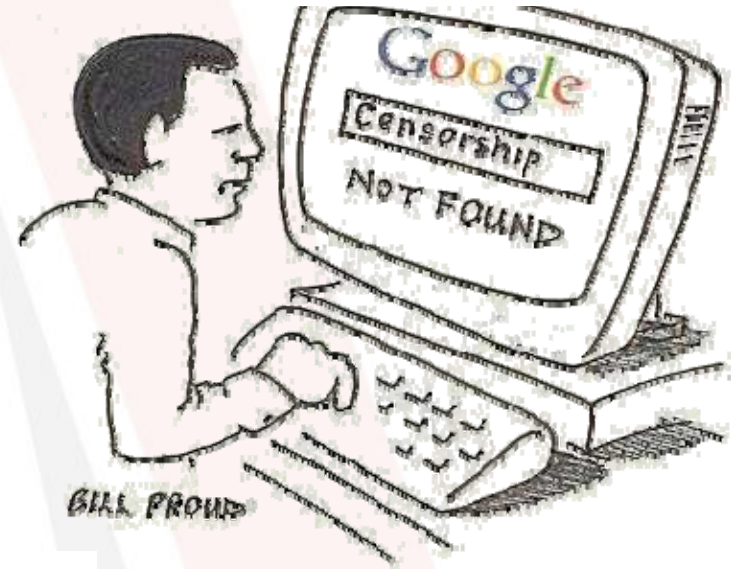
... and complete



Being too restrictive?

Usually when access to information is completely restricted, with the intention of protecting the information, you don't derive the benefit from the available technology and improved methods.

and this happens





People find a way around it anyway

Internet application usage has expanded dramatically—to the point where virtually all corporations have employees using at least one such application: survey results indicate that **97%** of end-users now use one or more of these Internet applications, up from **85%** reported last year.

[The Collaborative Internet: Usage Trends, End User Attitudes and IT Impact. Facetime, Oct 2008]

Industry estimates state that **60%** of corporate data resides on unprotected PCs and laptops, **10%** of laptops are lost or stolen in the first year of purchase, and **66%** of USB devices are lost or misplaced in their lifetimes

[Google, 2009. www.google.com/apps/intl/en/business/switch_benefits.html]

A December 2007 survey conducted by the Ponemon Institute found that 4 out of 10 employees reported losing a laptop, mobile phone, PDA, or flash drive containing company data.

In that same study, more than half of employees report copying sensitive information to flash drives, even though **87%** of those companies had policies prohibiting the practice.

[Survey of US IT Practitioners Reveals Data Security Policies Not Enforced," Ponemon Institute, 2007]



Build it and they will come ...

Some what connected people (Web 1.0)



Who know they should be more connected



So they get together to share information and collaborate



Web 2.0



Mobility & Access to Information: Agenda

- Market Drivers for Mobility & Web 2.0 Services
- Intro to Web 2.0 & Mobility
- Corporate Response - Permit or Deny
- **Current trends & relevance**
- Mobility Security Issues
- Web Application Security Issues
- Conclusion



Why should you care about Web 2.0?

Consumer (i.e. "Web 2.0") technologies are already finding their way into the enterprise.

- Employees use (sanctioned and unsanctioned) consumer tools to perform day-to-day business tasks
- Enterprise applications use consumer technologies to provide the latest and greatest in usability and functionality
- Examples include: instant messaging, blogs, mashups, wikis

.....and Web Applications are the focus of attacks

- Web applications in general have become the Achilles heel of Corporate IT Security.
- Nearly 55% of all vulnerability disclosures in 2008 affect Web applications
- SQL injection jumped 134% and replaced cross-site scripting as the predominant type of Web application vulnerability (several hundred thousand per day at the end of 2008).

[Source: IBM]



- 78% of IT organizations are concerned about the risks of employee-driven, unsanctioned use of Web 2.0 tools and technologies
- 50% of respondents said they "customize their work environment moderately or aggressively" (including the use of unsanctioned tools) and will continue to do so.

[Source: Forrester Research]

[Source: Gartner Research poll]



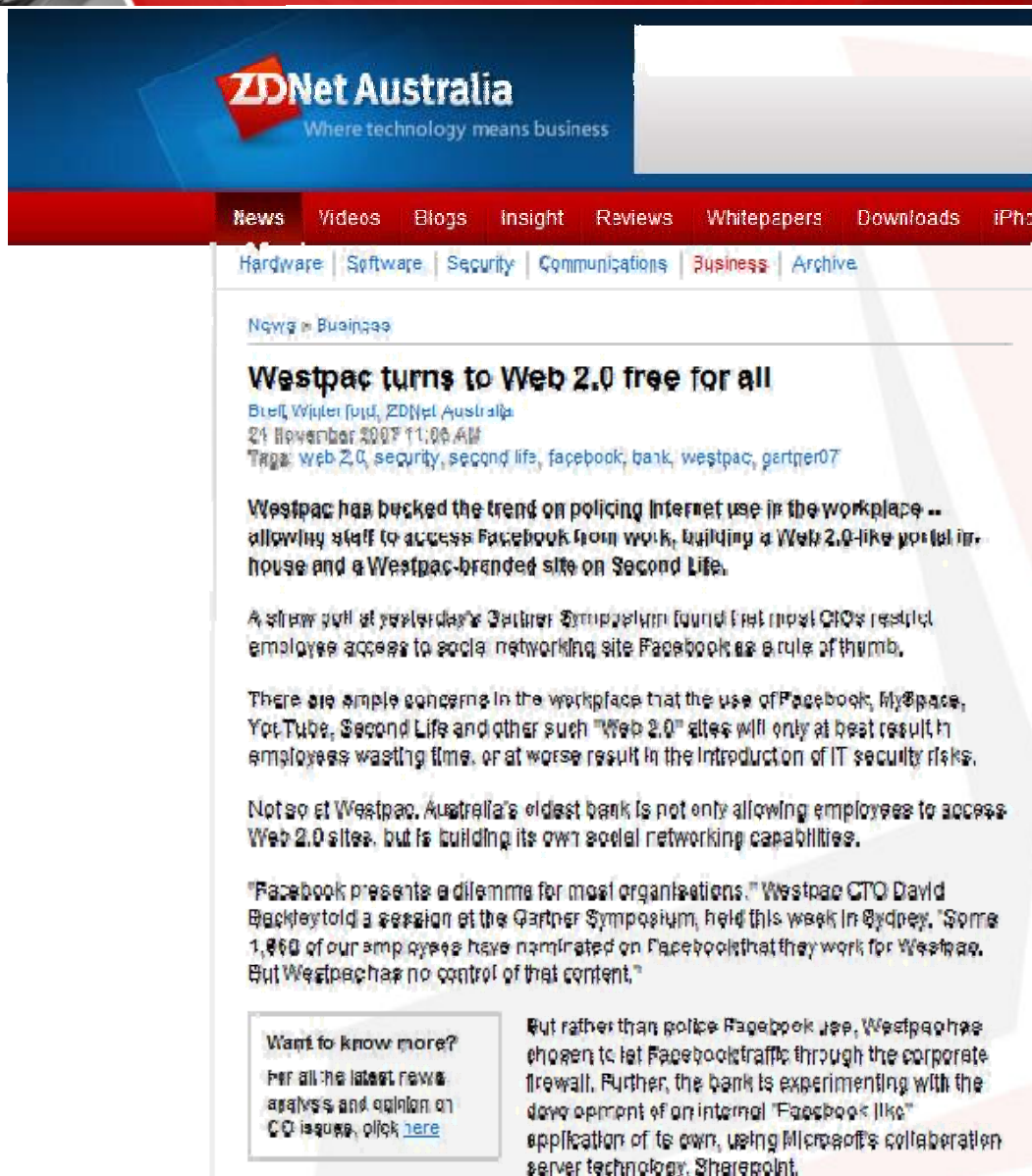
So how much information is out there?

- 487,000,000,000 Gigabytes of Digital Content Today to Double Every 18 Months (IDC, 19May09)
[<http://www.infoniac.com/hi-tech/digital-content-today-to-double-every-18-months.html>]
- 133,000,000 - number of blogs indexed by Technorati since 2002
- 900,000 - average number of blog posts in a 24 hour period
- 1,200,000,000 - number of YouTube videos viewed per day (Techcrunch 9Jun09)
- 20 hours - amount of video are uploaded to YouTube every minute (TechCrunch May09)
- 65,000 iPhone apps online; 1,500,000,000 downloaded and more than 100,000 developers (MX News, July 15)

[Ref: <http://thefuturebuzz.com/2009/01/12/social-media-web-20-internet-numbers-stats/>]



So some adopt it



ZDNet Australia
Where technology means business

News Videos Blogs Insight Reviews Whitepapers Downloads iPhone

Hardware Software Security Communications Business Archive

News » Business

Westpac turns to Web 2.0 free for all

By Jeff Wujcik (jw), ZDNet Australia
24 November 2007 11:00 AM
Tags: web 2.0, security, second life, facebook, bank, westpac, gartner07

Westpac has bucked the trend on policing Internet use in the workplace -- allowing staff to access Facebook from work, building a Web 2.0-like portal in-house and a Westpac-branded site on Second Life.

A straw poll at yesterday's Gartner Symposium found that most CIOs restrict employee access to social networking site Facebook as a rule of thumb.

There are ample concerns in the workplace that the use of Facebook, MySpace, YouTube, Second Life and other such "Web 2.0" sites will only at best result in employees wasting time, or at worse result in the introduction of IT security risks.

Not so at Westpac, Australia's oldest bank is not only allowing employees to access Web 2.0 sites, but is building its own social networking capabilities.

"Facebook presents a dilemma for most organisations," Westpac CTO David Backley told a session at the Gartner Symposium, held this week in Sydney. "Some 1,860 of our employees have nominated on Facebook that they work for Westpac. But Westpac has no control of that content."

Want to know more?
For all the latest news, analysis and opinion on CIO issues, click [here](#)

But rather than police Facebook use, Westpac has chosen to let Facebook traffic through the corporate firewall. Further, the bank is experimenting with the development of an internal "Facebook like" application of its own, using Microsoft's collaboration server technology, SharePoint.





And sometimes things go wrong

HORRIBLY WRONG



Sensitive information published online

Facebook: MI6 wife's photos

Posted by Laurel Papworth in Australia, Facebook, Online Communities, Rules of Engagement, Safety, blogs, government, social media, social networks, web 2.0 on 07 7th, 2009 | 2 responses

8

tweets

retweet

When people ask "why do young people post up photos of themselves drunk and throwing up at parties? Don't they know it will impact their job chances later on?", there are a number of responses. One is "they don't take the photo and upload it...their 'friends' do – control of our personal brand is gone!". I thought the Secret Service had follow up training for family? Or I have just read too much John le Carré From Times Online:

Digg

submit

Wife of Sir John Sawers, the future head of MI6, in Facebook security alert

Diplomats and civil servants are to be warned about the danger of putting details of their family and career on social networking websites. The advice comes after the wife of Sir John Sawers, the next head of MI6, put family details on Facebook — which is accessible to millions of internet users.

Lady Sawers disclosed details such as the location of the London flat used by the couple and the whereabouts of their three children and of Sir John's parents. She put no privacy protection on her account, allowing any of Facebook's 200 million users in the open-access London network to see the entries.

Lady Sawers' half-brother, Hugo Haig-Thomas, a former diplomat, was among those featured in family photographs on Facebook. Mr HaigThomas was an associate and researcher for David Irving, the controversial historian who was jailed



<http://laurelpapworth.com/facebook-mi6-wifes-photos/>



And even the technologists are affected

[Tech](#) [Gadgets](#) [Mobile](#) [Enterprise](#) [CrunchBase](#) [More](#)



[About](#) [Advertise](#) [Archives](#) [Company Index](#) [Contact](#) [CrunchCam](#) [Jobs](#) [Research](#)

Twitter's @Ev Confirms Hacker Targeted Personal Accounts; Attack Was "Highly Distressing."

by **Erick Schonfeld** on July 14, 2009 85 Comments



Evan Williams Wow, I can't believe that worked. Just bought saraishot.com via @tweename. (Was just testing; didn't expect it to be avail.) Nice, @pud! via Twitter - 16 hours ago

[Wall](#) [Info](#) [Photos](#) [Boxes](#)

Basic Information

Networks:	San Francisco, CA Odeo Twitter
Sex:	Male
Birthday:	March 31, 1972
Hometown:	Los Angeles, CA


[View Photos of Evan \(22\)](#)
[View Videos of Evan \(1\)](#)
[Send Evan a Message](#)
[Police Fun](#)

Back in May, **Twitter was hacked** by someone who got into the accounts of several Twitter employees and then gained access to high-profile accounts such as those of Britney Spears and Ashton Kutcher. The breach was the work of someone going by the name Hacker Croll, who posted the compromised screen shots on a French message board. Now more screenshots attributed to the same hacker have popped up on another **French site** (rough **translation here**).

According to the post, Hacker Croll was able to compromise the Twitter accounts of founder **Evan Williams**, his wife, and several employees. Using password recovery techniques, Hacker Croll claims he gained access to various Paypal, Amazon, Apple, AT&T, MobileMe and Gmail accounts. I emailed Evan Williams asking about the breach. He confirms:

Yes, we did suffer an attack a few weeks ago and are familiar with this list of stuff. This is unrelated to the hack of twitter where someone gained access to user's accounts. This had nothing to do with the security of **twitter.com**, and there were no user accounts

[Tech](#) [Gadgets](#) [Mobile](#) [Enterprise](#) [CrunchBase](#) [More](#)



[About](#) [Advertise](#) [Archives](#) [Company Index](#) [Contact](#) [CrunchCam](#) [Jobs](#) [Research](#)

Twitter's Financial Forecast Shows First Revenue In Q3, 1 billion users in 2013

by **Michael Arrington** on July 15, 2009 258 Comments

Our negotiations with Twitter (or rather Twitter's lawyers) over our **intention to publish** a small subset of the 310 hacked confidential documents continue. We published the first document, a **pitch** for a reality television show called Final Tweet, earlier this morning.

Far more interesting, though, is this internal Twitter financial forecast from February 2009. Twitter has told us that this was never an official document and it certainly is no longer accurate. But it gives an interesting glimpse into the company's financial targets nonetheless. The projections go forward to 2013.

The most interesting data point - As of February, Twitter expected their first revenue to come in Q3 2009 (which is now). A modest \$400,000 was expected, followed by a more robust \$4 million in Q4. The document also shows Twitter's projected user growth (25 million by the end of 2009), which it has absolutely blown through already. By the end of 2010, Twitter expected to be at a \$140 million revenue run rate.



A Must Read: <http://www.techcrunch.com/2009/07/19/the-anatomy-of-the-twitter-attack/>





Data copied to mobile devices and lost

Posted by Arianna | May 12, 2009 | 0 Comments

1 Million Affected After Laptop Stolen from Car

Related entries in Data Breach, Laptop Security, Real Theft Reports, Security Breach, Security Policy

Who Breached: Oklahoma Department of Human Services

Number Affected: 1 Million+

Information breached: Social Security Numbers

How: laptop stolen from car

It's been a while since I've done a major highlight of any recent data breaches. They keep happening, to be sure, but the details often start to look the same. However, this one caught my eye from its magnitude. The Oklahoma Department of Human Services (OKDHS) is notifying more than 1 million residents of the state that their data has been breached as the result of a stolen, unencrypted, laptop.

According to their press release, a password-protected OKDHS laptop was stolen from an employee's vehicle (a far too common theft location). The laptop contained names, Social Security Numbers, dates of birth and home addresses for clients who received Medicaid, Child Care assistance, and other program assistance. The laptop was stolen on April 2nd with a press release going out from OKDHS on April 23rd. Letters to affected clients started to go out in the same week.



<http://blog.absolute.com/category/security-breach/>



Analysts see alarming development in mobile malware

For the first time, a piece of mobile malware can send and receive information from a remote server

Jeremy Kirk (IDG News Service) 17 July, 2009 03:37:00

Tags: smartphones, security, mobile phones, mobile malware

The first worm that spreads between mobile devices by spamming text messages has developed a new communications capability that one security vendor says signals the arrival of mobile botnets.

Trend Micro has analyzed a piece of mobile malware known as "Sexy Space," which is a variant of another piece of mobile malware called Sexy View, which targets devices running the Symbian S60 OS.

Sexy View, which was detected by vendors such as F-Secure six months ago, is significant because it is the first known malware sample that spreads by SMS (Short Message Service). It appeared initially in China.

Infected phones would send SMSes to everyone in the phone's contact list with a link to a Web site. If someone clicked the link, they would then be prompted to install Sexy View, which purports to offer pornography-related content.

In another advancement, those who wrote Sexy View were able to get the application approved and signed by Symbian. The OS manufacturer, now owned by Nokia, vets applications for

Have your say!
Write a comment



Add to iGoogle

Print this story

Digg this story

More by Jeremy Kirk

ARN Directory | Distributors
relevant to this article

Brightpoint Australia , Cellnet ,
Corporate Computer Resources ,
ICT Distribution , Ingram Micro
Australia , itX , Leader Computers ,
NewLease , Techhead Connect ,
Westcon Group

ARN Directory | Vendors relevant to
this article

Trend Micro

More about mobile phones

- Does mobile tech breed narcissism?
- Verizon's exclusivity compromise: unimpressive gesture
- Sony Ericsson launches 8.1-megapixel camera phone

[More about mobile phones >](#)

[Ref: http://www.arnnet.com.au/article/311467/analysts_see_alarming_development_mobile_malware?eid=-217]



Mobility & Access to Information: Agenda

- Market Drivers for Mobility & Web 2.0 Services
- Intro to Web 2.0 & Mobility
- Corporate Response – Permit or Deny
- Current trends & relevance
- **Mobility Security Issues**
- Web Application Security Issues
- Conclusion



And why does it happen? Mobility

Adoption of mobility solutions requires enterprise security to be extended BEYOND the enterprise perimeter.

- There is no corporate policy
- The backdoor is left open with USB keys.
- The side entrance door is left open with the wireless network.
- Information is published (read LEAKED) to blogs/collaboration/info sharing sites.
- Laptops, removable media, mobile phones store vast amounts of sensitive data and are still seldom encrypted.
- Data in transit is seldom encrypted.
- Poor (if any) authentication to corporate data for mobile users.





5 Steps to Mobility Security

Policy

- Create a policy that covers the device lifecycle, from selection to recovery.

Data In Motion

- Encrypt all data over mobile and WiFi networks. Use VPN clients or application layer encryption.

Data at Rest

- Encrypt data stored on device. Manage cached data with 3rd party software and passwords.

Malware Protection

- Protect against malware with policy (Bluetooth, downloads) and technology (anti-malware SW).

Authentication

- Require user authentication at points required for acceptable risk/aggravation.

[Ref: Opus1, Five Steps To Securing Mobile Devices, 2008]





Mobility & Access to Information: Agenda

- Market Drivers for Mobility & Web 2.0 Services
- Intro to Web 2.0 & Mobility
- Corporate Response - Permit or Deny
- Current trends & relevance
- Mobility Security Issues
- **Web Application Security Issues**
- Conclusion



And why does it happen? Web Collaboration

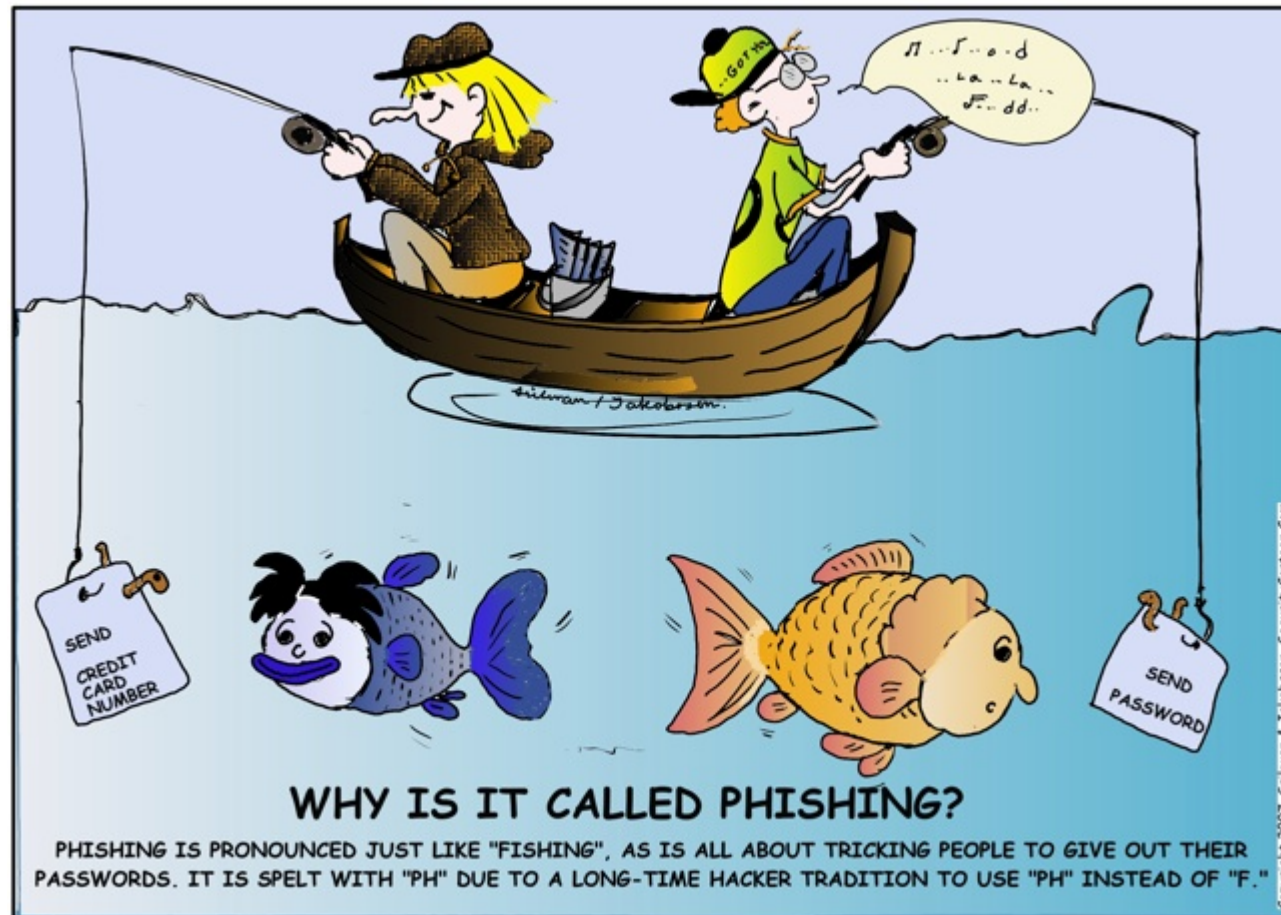
Social:

- Too much personal information online
- Very grey lines about what is private
- Changes with demographic

Result:

- Easier social engineering attacks...
- Sensitive information inadvertently published (MI6 example shown earlier)

Credentials are gold



"Reproduced with permission. Please visit www.SecurityCartoon.com for more material."



So they can

Take your money



Or sell your data to make
money





TMI: Too Much Information

Snapshot study: Mint (www.mint.com)

- An online free web application helping users with managing their money and budgeting
- Downloads, categorises, and graphs all of your finances automatically every day
- Users are required to supply their account credentials including pins and passwords (Read only access for analysis only)
- Over 1 million users (Jul 2009)
- Adding over 3,000 users every day
- Connects to more than 7,500 US financial institutions
- Mobile Access – Mint for iPhone
- Mint does not offer terms and conditions that guarantee anything. You provide them with Power of Attorney. You indemnify them against all claims. Mint is not responsible or liable to you.





Mint continued ...

- The usernames and passwords you use to access your online financial accounts are not viewable by Mint.com employees or contractors.
- This information is collected from you one time only in order to establish a persistent connection to your financial institutions.
- Your credentials are encrypted and securely passed to our online service providers who maintain them in order to deliver your transactional data to the Mint service.
- The information is never stored on the Mint.com site

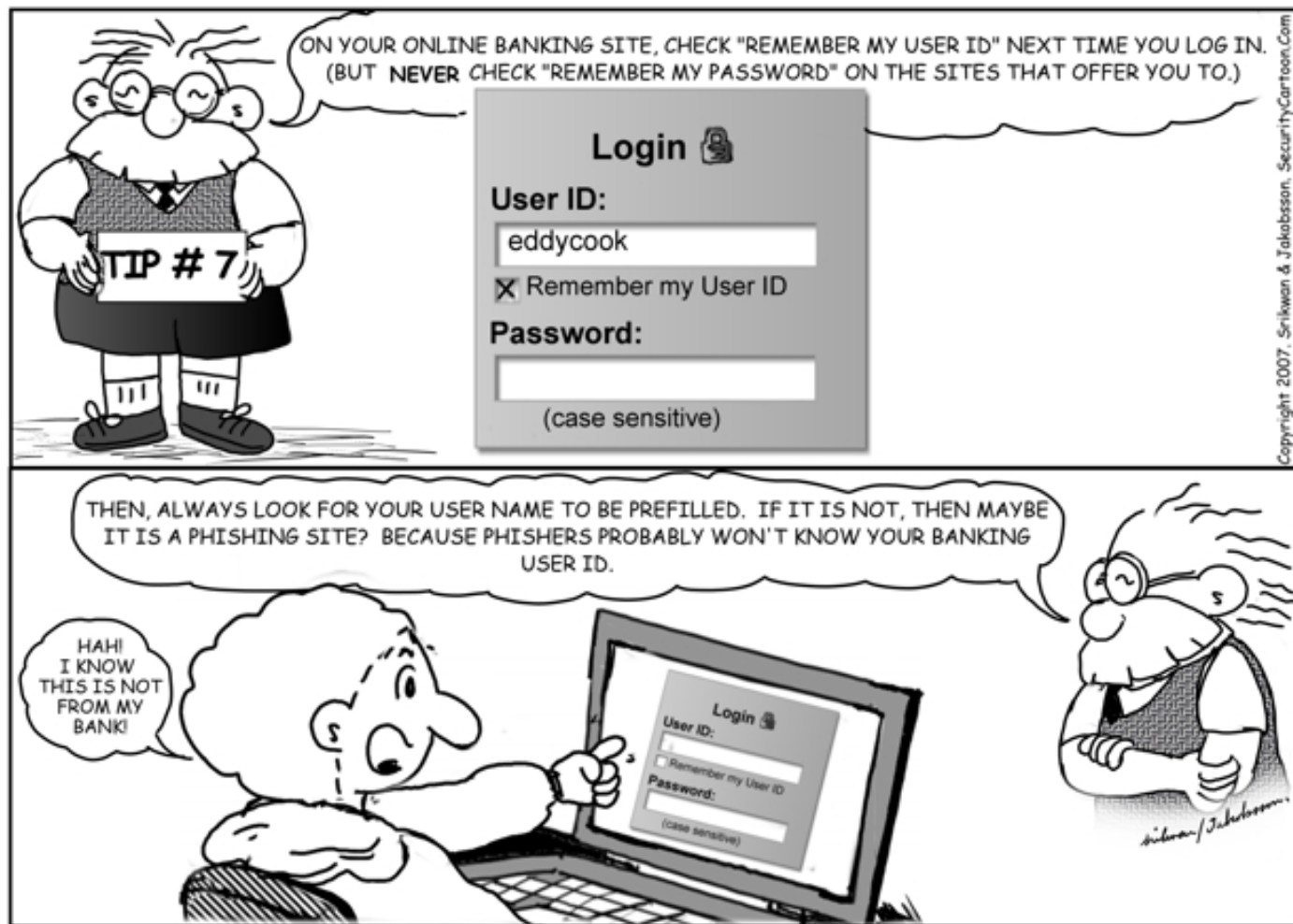
BUT

- On their own forum site they selectively answer questions
- Ask any question as long as they have a marketing style answer for it
- Some serious posts about viewing someone else's account information ignored

Sounds like a good idea but perhaps not quite there yet



"Remember Me" functionality



Impact: Increases the possibility of cross-site scripting & similar session hijacking attacks

"Reproduced with permission. Please visit www.SecurityCartoon.com for more material."



Password Security \$%^@!@#\$\$@#\$\$

- Many applications limit password length and complexity!
- So even if users try to adopt good password measures they can't.
- This forces the user to be insecure.



- Why do so many sites not enforce SSL Logon?
- Even if SSL Logon is enforced - may still succumb to threats.
 - Ref SSLStrip tool. Redirects through ARP Spoof and creates a MITM attack.
- Always check server certificate.



Web 2.0 Security Trends

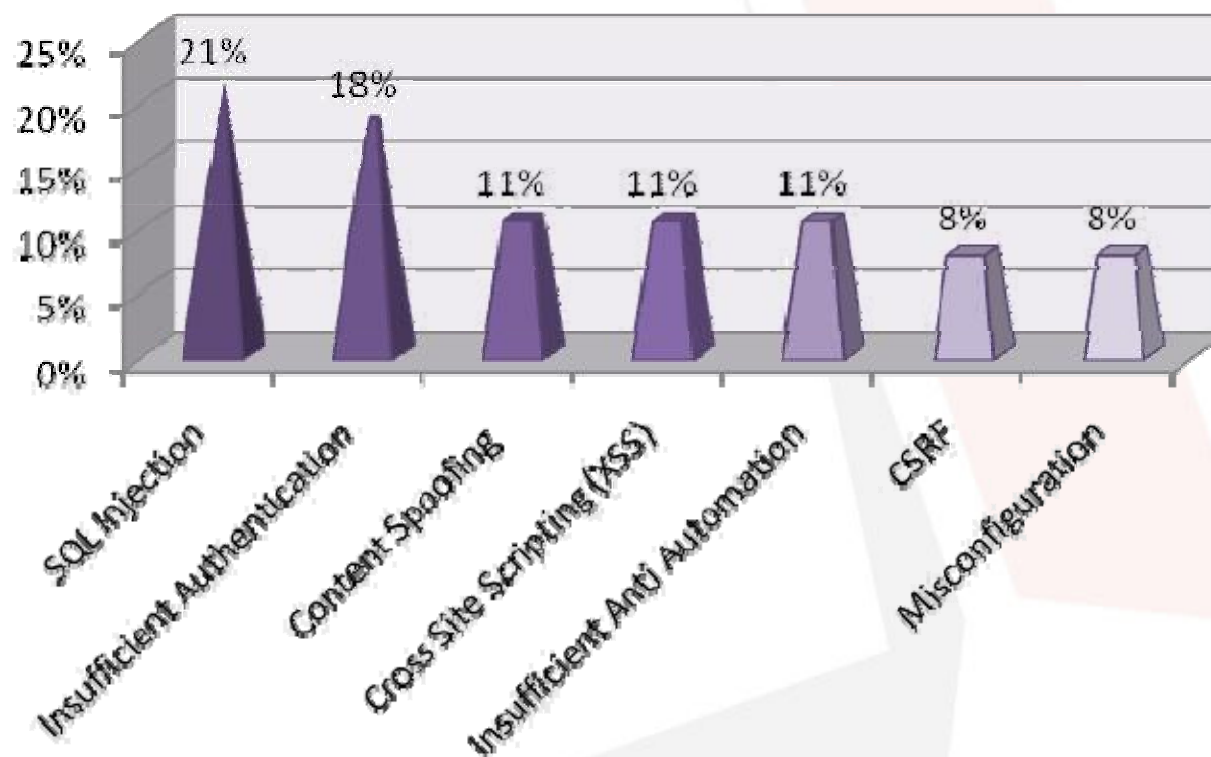
According to a recent report based on analysis of recent “web hacking incidents of importance” it is concluded that :

- Web 2.0 services and sites lead the list with highest number of all recorded incidents (21%).
- Most popular attack vectors exploiting Web 2.0 features are SQL injection (21% of attacks) and Authentication abuse (18%). A new emerging threat is Cross Site Request Forgery (CSRF) that currently ranks as the 6th most popular attack vector with 8% of the reported attacks.
- Leakage of sensitive information remains the most common outcome of web hacks (29%), while disinformation follows with 26%, mostly due to hacking of online identities of celebrities.

[Ref: Secure Enterprise 2.0 Forum; WEB 2.0 HACKING INCIDENTS & TRENDS 2009 Q1]

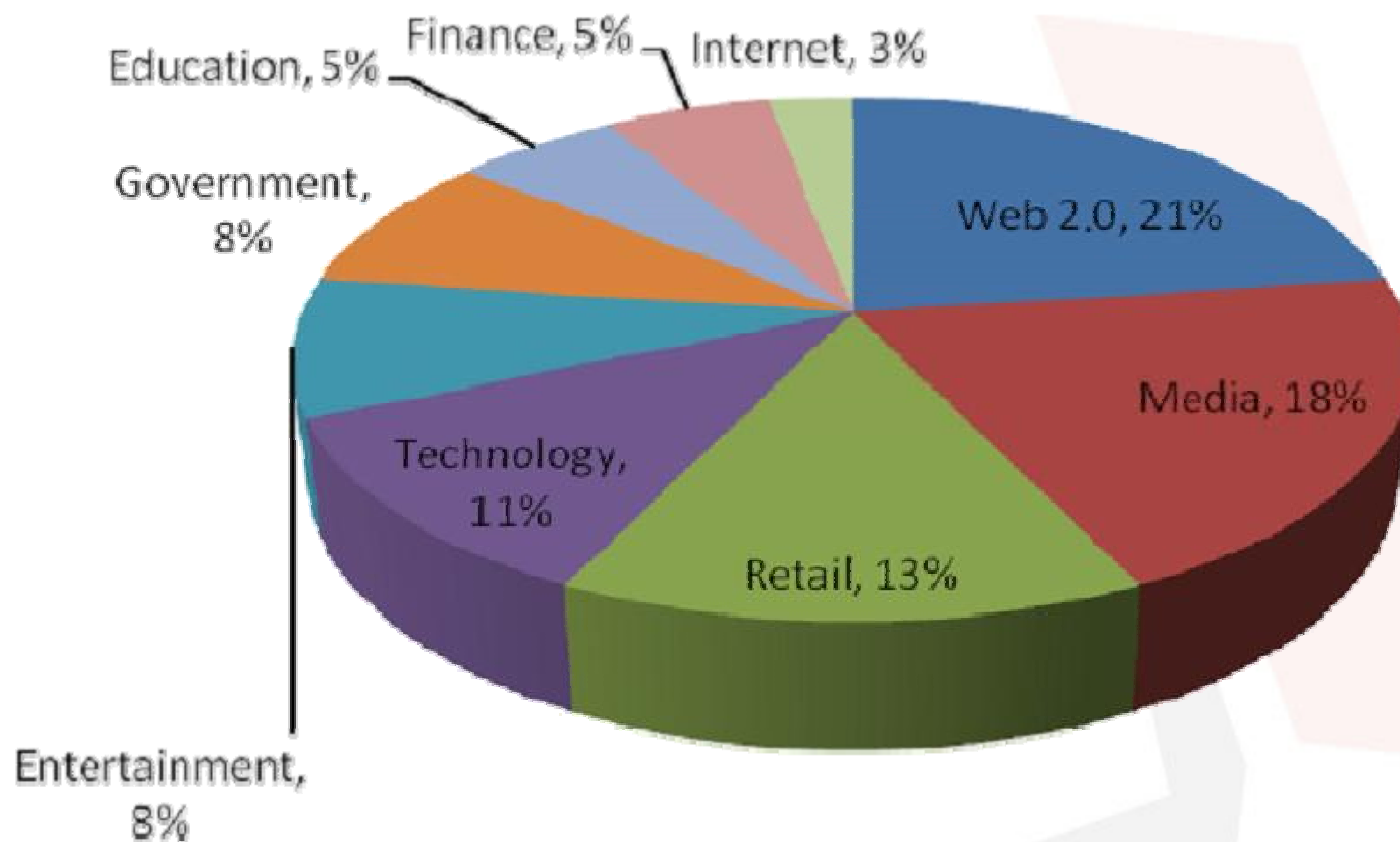


Web 2.0 is different but still the same



[Ref: Secure Enterprise 2.0 Forum; WEB 2.0 HACKING INCIDENTS & TRENDS 2009 Q1]

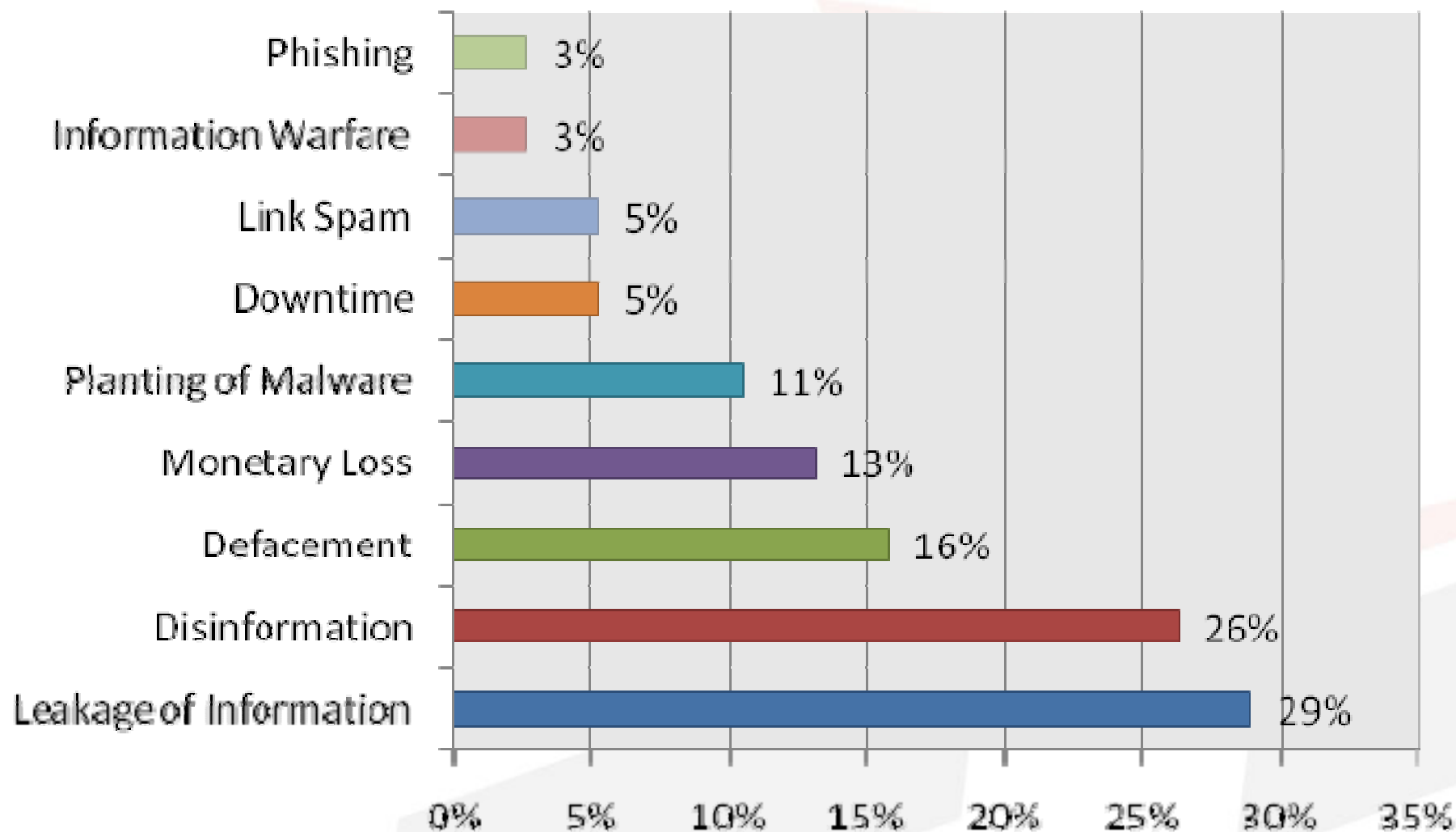
Who is being attacked?



Speaker's Note: Sample size unknown. This sample may not accurately represent the Australian landscape.

[Ref: Secure Enterprise 2.0 Forum; WEB 2.0 HACKING INCIDENTS & TRENDS 2009 Q1]

What is motivation/outcome of attack?



[Ref: Secure Enterprise 2.0 Forum; WEB 2.0 HACKING INCIDENTS & TRENDS 2009 Q1]





Key steps to web application security

If Developing

- Develop Securely. Use Secure Coding Guidelines. Ref OWASP
- Run Vulnerability Management Lifecycle Program. Complement with frequent penetration tests.

If using 3rd party

- Review security measures in place.
- Understand how your information is secured.
- Review and understand T&C's of the service.

Firewalling

- Use Web Application Firewalls and Application/Protocol firewalls.
- Traditional network firewalls over no protection.

Engage with experts

- Understand threat landscape.
- Perform technical and business aligned security reviews





Mobility & Access to Information: Agenda

- Market Drivers for Mobility & Web 2.0 Services
- Intro to Web 2.0 & Mobility
- Corporate Response - Permit or Deny
- Current trends & relevance
- Mobility Security Issues
- Web Application Security Issues
- Conclusion

- Web 2.0 is both a set of technologies as well as a new set of consumer behaviours.
- The interactive internet is growing daily and here to stay.
- Those who do not adopt these emerging technologies will eventually be left behind.
- Attacks against web applications are on the increase. Protect yourself against all attack vectors. Review web applications frequently.
- Data Loss will continue to plague organisations. Know where and what your data is and encrypt it in motion and at rest.
- Effective mobility solutions are required to deliver cross platform, multi vector access to web applications.
- You can find the balance between



and





Thank You

Thank You

Murray Goldschmidt - General Manager

Sense of Security Pty Ltd

Tel: +61 2 9290 4444

info@senseofsecurity.com.au

www.senseofsecurity.com.au

Sense of Security is an endorsed supplier to the
NSW Government ICT Services Panel (2020) for Whole of Government

