

M86 Security

Is Your AUP Social Media Proof?

August 2010

Today's Speaker



- Bradley Anstis
- Vice President, Technical Strategy, M86 Security
- Speaker on security technology and malware trends
- Over 20 Years of IT industry experience

Agenda

- What is an Acceptable Use Policy (AUP)?
- Why Do You Need An AUP?
- Why Do I Need to be Concerned about Social Media?
- Steps to Consider When Creating and Developing an AUP
- How to Make your AUP Social Media Proof
- M86 Solutions that Help Enforce Your AUP

Acceptable Use Policies (AUP)



What is an Acceptable Use Policy?

- An organization's policy on how its email & Web resources should be used
- Typically signed by new employees at induction
- Usually covers:
 - Work related and personal use of IT equipment as well as behaviour or conduct
 - Description of acceptable language in communications
 - Description of acceptable images
 - Description of acceptable use of Internet, e.g. No joke emails, no accessing adult content etc.
 - Explanation of what action will be taken should an employee breach these rules

How Can AUPs be Enforced?

- Was one of the initial drivers for content security solutions running on email and later Web gateways
- Content security can enforce these policies consistently across all employees and provide the notification/reporting elements desired
- Example controls:
 - Inappropriate language filters
 - Inappropriate image analysis
 - Dangerous file types
 - Inappropriate Web sites
 - Overuse of non-work related Web browsing activity
 - Overuse of non-work related email



Why Do You Need an AUP?

- Safe Working Environment
 - In most jurisdictions it is the organization's responsibility to provide a 'Safe Working Environment'
 - This means protecting the employees as well as limiting the legal liability risk to the business
 - Aggrieved employees can sue the organization for failure to comply to regulations and legislations; even though another employee may be at fault and not the business. This can be incredibly expensive!
 - Content security filtering can be seen as a defence to protect a business and reduce the risk of legal exposure



Why Do You Need an AUP?

- Employee Productivity
 - Productivity can be a big issue with employees that have minimal oversight and fast internet connections and there are two effects to this
 - Are they as productive as they can be?
 - Are they choking Internet bandwidth that hinder other users or departments to do their job?



Why Do You Need an AUP?

- Internet Security

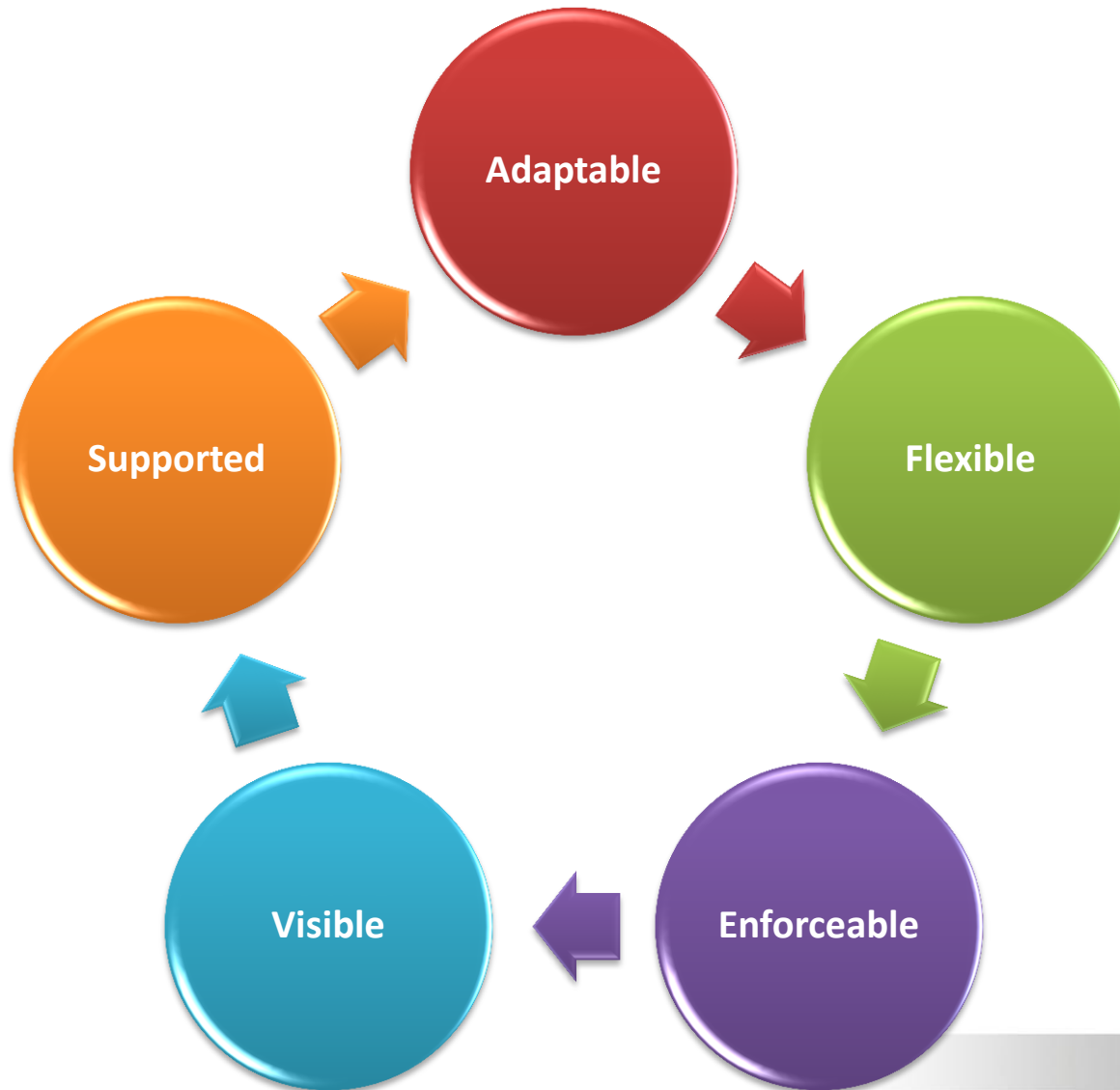
- Internet security covers two areas. The security of an organization's IT infrastructure and as well as the personal security or protection of employees
 - The Internet Threat Landscape is more dangerous and sophisticated than ever before, it is mandatory that organizations reduce their security exposure by care managing employees Internet use
 - The attacks and threats can either be targeted at an organizations information and resources or at individuals, compromising their identity and financial assets
- Trade-offs sometimes need to be made in competing areas



Steps to Consider when Creating and Developing an AUP

- There is no 'one size fits all' AUP. Organizations will need to customise their own to suit all requirements
- A typical AUP should cover these areas:
 1. Allow limited personal use of Web and email
 2. Outline what is acceptable and what is not; while preserving company culture
 3. Be consistent with enforcement and setting precedents
 4. All email should be identified with a name or email address – to avoid spoofing
 5. Inform staff on Copyright issues relating to email or Internet documents
 6. Monitoring and enforcement; inform staff about what is acceptable inside business hours and what is acceptable outside of business hours, if there is any difference. This needs to be clearly stated in the policy.
 7. Reserve the right to monitor all messages/files on the company network

Considerations when Creating an AUP

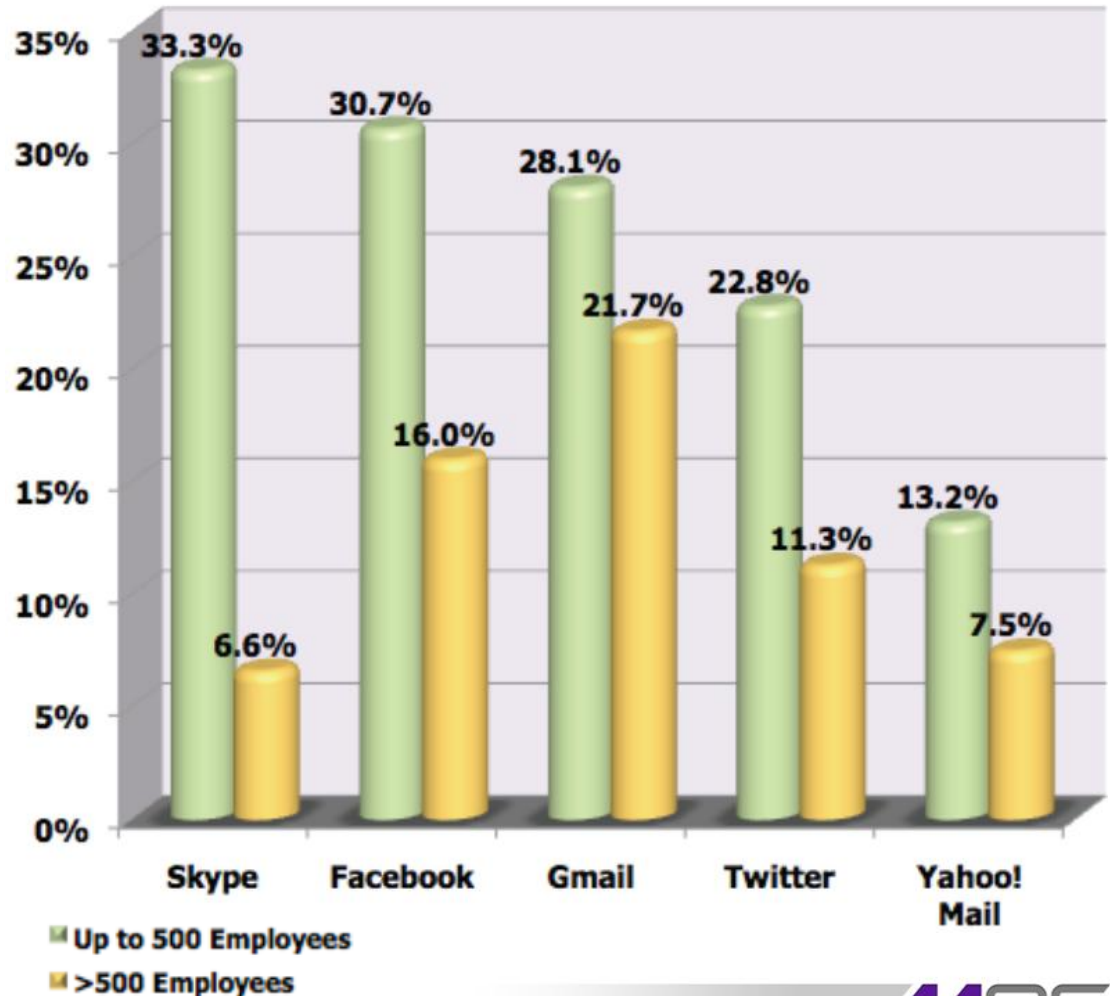


Why Do You Need to be Concerned about Social Media?

Adoption is Accelerating Quickly

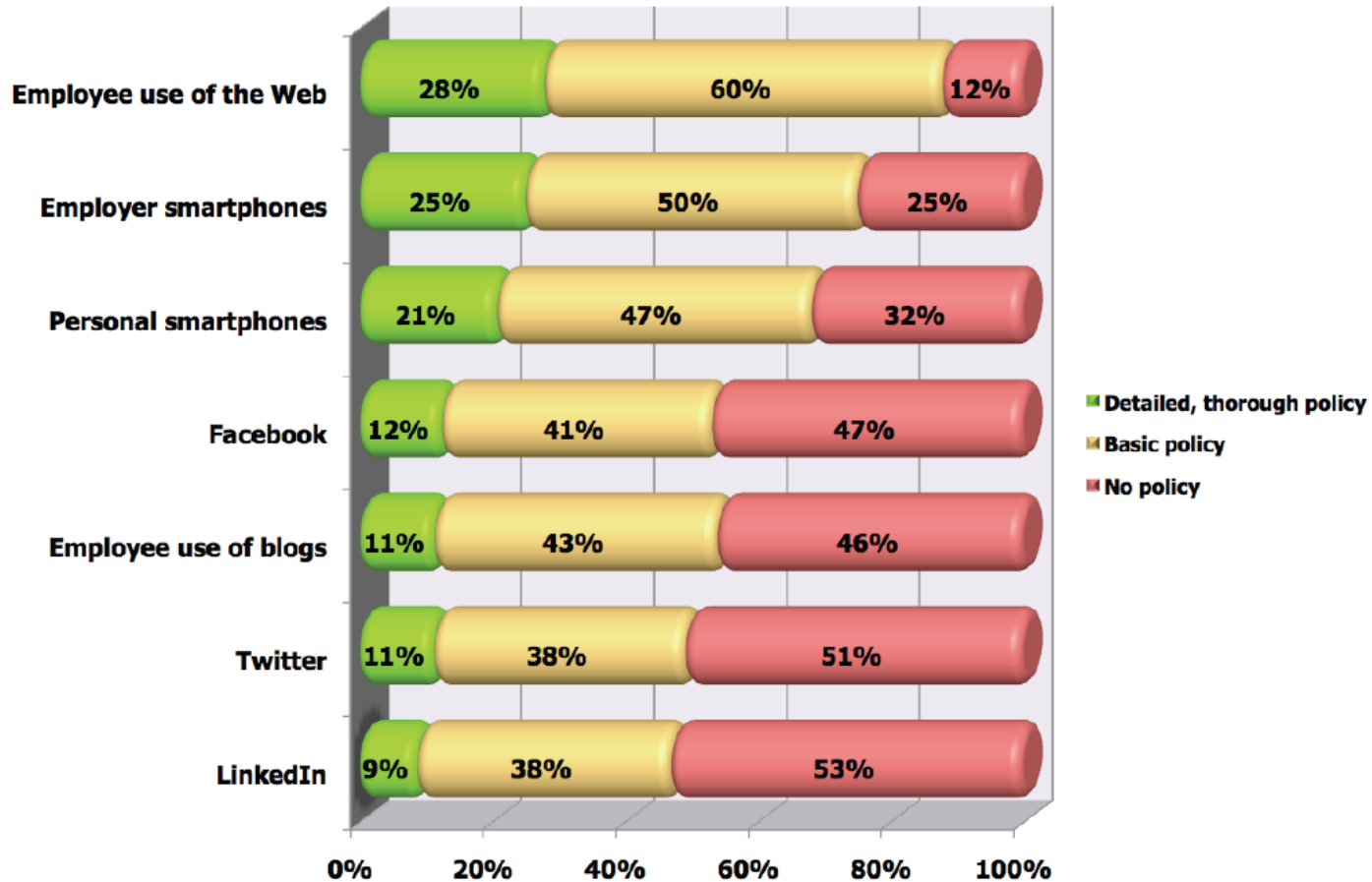
Use of Various Web 2.0 Tools

- In April 2010, 110 billion minutes were spent on blogs and social networking pages
- In April 2010, Blog and Social media sites attracted 24% more visitors than a year earlier
- There are currently 190m Twitter users, 519m Facebook, 65m LinkedIn and 115m on Friendster



State of Current Policy Controls

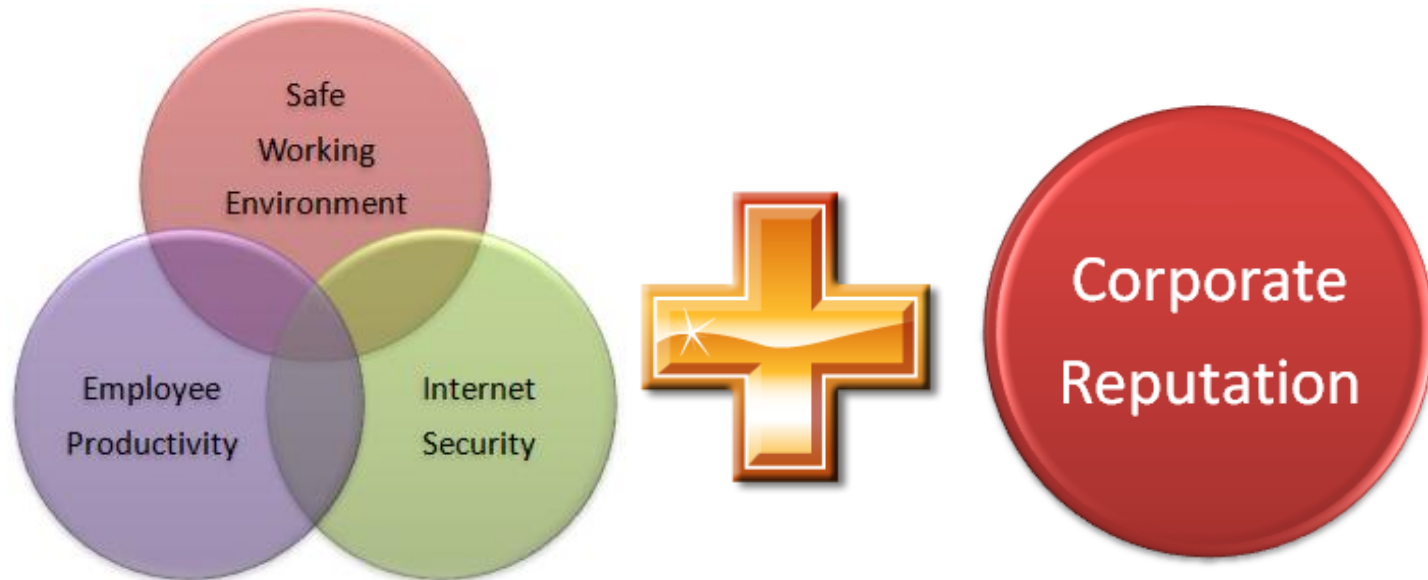
Current Organizational Policies for Various Communication Tools



Source: The Benefits and Risks of Web 2.0', Osterman Research, 2010

Why include Social Media in Your AUP?

- Organizations have always been concerned about brand reputation but the ease of access, difficulty of retraction of typically un-filtered social media communication has taken this concern to a new level
- Therefore, use of Social Media must be added to today's AUP as a core component



Example of Reputation Damage from Social Media

In January 2009, an employee of public relations firm Ketchum used Twitter to post some very unflattering comments about the city of Memphis shortly before presenting to the worldwide communications group at FedEx – Memphis' largest employer. An employee of FedEx discovered the tweet, responded to the tweeter, and then copied FedEx's senior managers, the management of FedEx's communication department and the powers that be at Ketchum.

A senior manager at FedEx responded to this post with the following: “....everyone participating in today's event, including those in the auditorium with you this morning, just received their first pay check of 2009 containing a 5% pay cut...many of my peers and I question the expense of paying Ketchum to produce the video open for today's event; work that could have been achieved by internal, award winning professionals with decades of experience in television production.”

<http://shankman.com/be-careful-what-you-post/>

Example of Reputation Damage from Social Media

Last week a homophobic Vodafone UK employee wrote the following message on its official Twitter account: "VodafoneUK is fed up of dirty homos and is going after beaver".

The Guardian newspaper reports this nasty tweet prompted hundreds of users to contact the company to complain. The firm later issued the following press release indicating the message originated from a rogue staff member:

"This afternoon an employee posted an obscene message from the official Vodafone UK Twitter profile.

"The employee has been suspended immediately and we have started an internal investigation. This was not a hack and we apologise for any offence the tweet may have caused."

The employee faces almost certain dismissal for gross misconduct.

<http://blogs.findlaw.com/solicitor/2010/02/homophobic-employee-causes-vodafone-severe-twitter-embarrassment.html>

Do You Know What You Are Doing?

UK Conservative party launched a website meant to expose the relationship between the then UK Prime Minister, Gordon Brown and a major UK Union, the conservatives were hoping that visitors to the site would use social media to spread the information further, but due to a missing security control on the site hackers were easily able to re-direct visitors to other websites including hard pornographic websites.

<http://www.telegraph.co.uk/technology/twitter/7499228/Conservatives-embarrassed-as-hackers-exploit-loophole-on-anti-union-website.html>

Search engines do not help by index all content including conversations between parties that an unintended party can view, privacy settings are vital

Make Your AUP Social Media Proof

Existing Web AUP?

- Create or Update your AUP
- Basis of Social Media AUP

Acceptable Behavior

- Acceptable Language or Images
- Acceptable Communications

Which Sites?

- Allow Approved Networks only?
- Allow all sites during certain times?

Separate Networks

- Professional/Work-related network
- Social/Non-work related network

Privacy Settings

- For any corporate profiles carefully review all privacy settings available
- Consider educating users on the importance of privacy settings and provide guidance for different sites

Acceptable Activity

- Allow all users to post data?
- Limit during work hours?

Allowed Plug-ins

- Users allowed to install games etc in profile?

- Check existing AUP's
- Do you have a Business Conduct Guidelines document?
- Investigate the sites your organization wants to use, what do the employees want?
- Consider asking employees to separate their social networks
- Very Important, clearly understand and set all privacy settings, particularly for the organizations profiles

M86 Security Solutions to Enforce Acceptable Use Policies

Strong Foundation

Current M86 Security Products



Real-time Security for the Borderless Network

Products

Web Security

Anti-virus
Malware Detection
Application Control

Messaging Security

Anti-virus
Malware Detection
Outbound Security

Reporting

Granular Reporting
Real-time Monitoring

Compliance

Encryption
Data Loss Prevention
Archiving

- Secure Web Gateway
- Web Filter

- MailMarshal SMTP
- MailMarshal Exchange

- Security Reporter
- MRC

- Product Suite

Deployment Options



Appliances



Software



Cloud Service (SaaS)



Questions?

<http://www.m86security.com/resources/webinars.asp>

http://www.m86security.com/documents/pdfs/white_papers/business/WP_Creating_And_Managing_Effective_AUPs.pdf