

# Social media and its security in corporate environments

By Kevin Fitzgerald  
Fitzgerald InfoSec

1

Commercial in Confidence

© Fitzgerald InfoSec

## Executive Summary

- It can be expected that Social Media will make its way into corporate life increasingly over the next few years. It will eventually become as common as mobile telephone usage today presenting both opportunity and risk to corporate and government organisations.
- It is essential that corporate and government organisations understand those elements of social media that are capable of making positive contributions and those that may make negative contributions to their business.
- Positive contributions must be defined, evaluated for suitability and once accepted, harnessed effectively.
- Negative contributions must be assessed through Risk Management and Analysis and appropriate control objectives applied and implemented.
- The major risks, as usual, will be people-related not technical-related, so it is essential that the behaviour rules for people are clear and enforced.
- A Social Media usage Policy, Standards and Guidelines must also be developed and signed off by executive and operational management as well as all personnel.

2

Commercial in Confidence

© Fitzgerald InfoSec

## What is Social Media (SM)?

- Easy access devices and platforms that allow easy social access and sharing:
  - Mobile telephones – voice, sms, mms, contact lists, appointments, calendar ...
  - Smart mobile telephones – inclusive of the above plus remote email access, Internet browser, Twitter, Navigator, Instant Messaging ...
  - Laptops - Face-book, Twitter, YouTube...
  - iPods – music
  - Web sites – Micro-blogging, Blogging, On-line Forums, Wikis, Podcasts and RSS feeds
  - Web 2.0 – web apps that facilitate interactive file sharing and collaboration on WWW. A Web 2.0 site allows users to create content rather than just read content.

3

Commercial in Confidence

© Fitzgerald InfoSec

## Expectations of Social Media's corporate entrance

- The likelihood that X and Y-genners (the Attention Agers) can exist without social media at work seems remote.
- A blurring of ownership will occur - employee owned devices (e.g. iPhones, laptops,) containing enterprise information.
- A blurring of loyalties - using company time for personal interests – mobile telephone and Facebook and using unsupervised personal time (at home) to do company assignments.
- Keeping Facebook, Twitter and other common Web 2.0 sites out of the organisation is futile. Young employees will expect to use them and to be able to share information easily.
- Security expectations must step up to provide guidance now.

4

Commercial in Confidence

© Fitzgerald InfoSec

## Guidelines for secure use of SM

- Understand the risks:
  - Positive risks –
    - Opportunities are ignored or not implemented successfully, e.g. in –
      - recruitment,
      - collaboration,
      - research,
      - brand expansion and consumer research.
  - Negative risks –
    - malware, phishing, spoofing,
    - Social engineering, impersonation, blackmailing from malicious outsiders,
    - Denial of Service attacks and security failures,
    - legal issues concerning privacy, data leakage and inability to reproduce evidence of SM communication/correspondence.

5

Commercial in Confidence

© Fitzgerald InfoSec

## Risk Management of exposures

- Developing a Risk Exposure profile for Social Media (as planned for your organisation) is essential to understand the problem.
- Involve both the positive and the negative risks to develop a Threat-Asset matrix which can approximate threat likelihoods and impacts over each relevant asset. The resulting risk exposures can then be ranked to create a Risk Exposure Profile.
- Develop a scatter diagram of the exposures and apply controls consisting of a mix of avoid, deter, prevent, detect, recover, insure and accept strategies.
- Apply the controls and create a Risk and Mitigation Management Register.

6

Commercial in Confidence

© Fitzgerald InfoSec

## Personnel must be given clear leadership in relation to use of SM

- The Information Security manual must be given a new chapter – “The Secure Use of Social Media – at work and at home.”
  - Each SM platform must be identified and appropriate Policies, Standards and Guidelines produced, published and promoted.
  - Clear and fair SM penalties and SM related Key Performance Indicators must be detailed for acceptance by all personnel.
  - Such SM penalties and KPIs must be reviewed at induction, appointment, training, promotion and performance reviews.
  - Amongst these policies, standards and guidelines must be reference to the organisation’s expectations in relation to the use of SM for private use during working hours and the security requirements for the use of corporate or personal computing facilities at home on corporate business.

7

Commercial in Confidence

© Fitzgerald InfoSec

## The future

- Organisations must continue to recruit young people to grow their business.
- Young people today belong to the “Attention Age” and will soon replace current managers that belong to the “Information Age”.
- Those from the Attention Age, who share information content freely and instantly, will be required to adopt the discipline of security. This will require careful management to ensure that the benefits of security does not affect the happiness of recruited talent.
- Organisations will be pulled into the Attention Age by these budding new leaders. All organisations will need to be open to change to take advantages of the new ways of growing a business and of attracting and retaining the new talent as it emerges from Attention Age business schools without placing their organisations at undue risk.
- The tools and platforms as well as the risks of the Attention Age will continue to evolve just as they have in the Information Age. As usual, business will need to remain vigilant to balance the advantages with the risks. But Social Media is here to stay.

8

Commercial in Confidence

© Fitzgerald InfoSec