

Developing policies and procedures

42



Develop policies & procedures




43



44



45

 Elements of policy & procedure

Standard

- Title
- Purpose
- Revision History
- Effective Date
- Persons affected
- Definitions
- Responsibilities

Change to suit risk appetite

- Policy
- Procedures

46

 Draft Policy – Very Low

For a very low risk appetite

- In recognition of the very high impact that online social networking activities have upon the business activities of XYZ Pty Ltd, XYZ Pty Ltd implements very strict restrictions on the use of online social networking activities by employees using XYZ Pty Ltd equipment, and/or making reference to the business of XYZ Pty Ltd.
- XYZ Pty Ltd emphasises procedural controls, regular and intense monitoring to online social networking activities referring to the business of XYZ Pty Ltd, and provides explicit guidelines to follow in responding to such activities.

47

 Draft Policy – Very High

For a very high risk appetite

- As online social networking activities have minimal impact upon the business activities of XYZ Pty Ltd, XYZ Pty Ltd provides some guidance in the use of online social networking activities by employees.
- Responses to online social networking activities that refer to the business of XYZ Pty Ltd are made on a case by case basis as XYZ Pty Ltd becomes aware of them.

48



Tailoring your procedures

Tailored procedures

- Refer to appendices for a process to tailor your response in line with the business's risk appetite

Workshop exercise

- Are there other possible actions a business could include in the procedure?
- Identify pros and cons for each suggested action

49



Acceptable online social networking activities

Possibilities

- Could ban all mentions by employees
- Could ask for pre-approval of a comment
- Could allow employees to publish, but have marketing manager subscribe to RSS feeds and have employees agree to make changes if requested
- Only have authorised representatives respond online
- Could block online social networking websites in work hours (but please be realistic)

50




Staff training and awareness program

Possibilities

- Content
 - Awareness of acceptable online social networking activities
 - Core principles in ensuring the privacy of personal information in an online environment
 - Specific training on the use of major identified online social networking websites to ensure privacy.
 - Practical advice in the use and etiquette of online social networking tools, including the use of email
- Make your requirements part of induction program, perhaps with an exam
- Require existing staff to attend annually, and perhaps pass an exam

51

 Online reputation monitoring

Possibilities

- Engage online reputation monitoring service provider
- At least set up Google Alerts!
- Document risky mentions in monthly, quarterly, or annual online *social networking references report*
- Subscribe to likely private online forums
- Ensure that applicants for positions are aware that the candidate's online profile may be examined in the course of assessing the candidate's suitability for the position.

52

 Responding

Possibilities

- May need to have lawyers involved
- For an employee, the HR manager would deal with it
- Core principles:
 - Demonstrate an interest and respond online to address a grievance, and be transparent about it
 - Never post an immediate, negative, response to an online reference. Have a conversation in person at a senior level
 - Legal action considered
 - Making no response may be the least harmful
 - All responses conducted professionally and honestly
- Monitor and document responses in *social networking references report*

Leverage business opportunities through OSN

53



Business opportunities and OSN

Qi
applied insight

54



Qi
applied insight

Are there opportunities?

Workshop exercise

- Identify other opportunities presented by online social networking

55



Research and development

Brand monitoring

- Understand the reach and impact of your brand
- Know what is being said in the 'hearts and minds' and be more reactive

Research communities

- Share and build ideas within internal and external communities to test their value

Innovation communities

- Users can provide recommendations for new features
- Communities of users can vote on new features to guide product or feature development

56



Marketing

Blogs

- Promote and discuss on your own blogs
- Get a groundswell of discussion amongst your customers

Communities

- Build relationships between users and the company products

Video on user-generated sites

- Viral marketing promotion
- Audience gives more weight to genuine user experiences than paid TV spots

57



Sales

Social networking sites

- Can target sales (but need to be careful!)
- Create groups & events e.g. Friends of Ford

Brand ambassador programs

- Identify loyal customers who bring others into your community

Communities

- Understand and target sales

Embeddable widgets

- Users can prove brand loyalty
- Points of presence for sales

58



Customer support

Support forums

- Customers can answer their own problems online
- Customers can help each other
- Become aware of issues much sooner
- Proactive support e.g. Direct2Dell

Wikis

- Customers can answer their own problems online
- Self-documenting
- Save on publishing costs and corrections

59



Operations

Internal social networks

- Cross-fertilisation of ideas
- From front line to back office – e.g. Blue Shirt Nation (Best Buy Inc)
- Promote the sense of culture and can bring together widely dispersed/loosely coupled workforces

Wikis

- Provides a platform to develop self-organising teams
- Take on responsibility and change

External social networks

- Leverage employees' networks to hire new staff

60



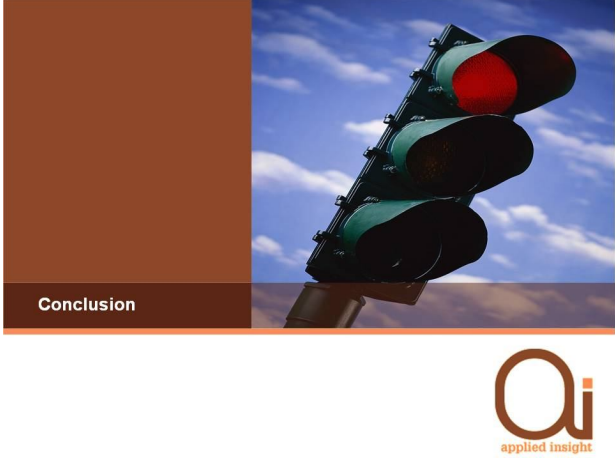
Cultural change

Recommendations for implementing

- Accept the loss of control
- Expect pushback from managers
- Line up executive backing
- Start small and focus on measurable objectives
- Expand beyond projects
- Stay focussed on culture, not technology

Conclusion

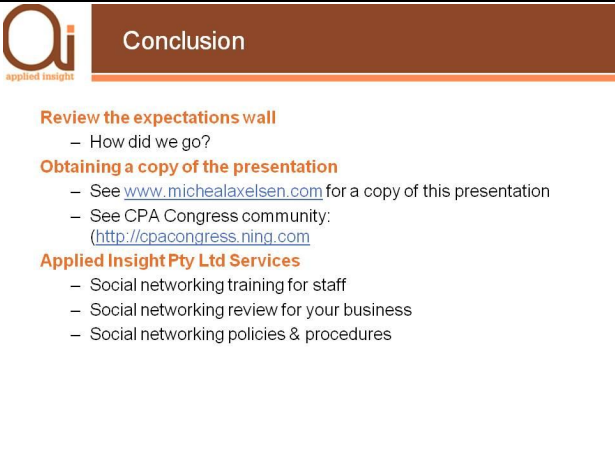
61



Conclusion

ai
applied insight

62



ai
applied insight

Conclusion

Review the expectations wall

- How did we go?

Obtaining a copy of the presentation

- See www.michealaxelsen.com for a copy of this presentation
- See CPA Congress community: (<http://cpacongress.ning.com>)

Applied Insight Pty Ltd Services

- Social networking training for staff
- Social networking review for your business
- Social networking policies & procedures

63



Contact details

Micheal Axelsen
Director, Applied Insight Pty Ltd
m: 0412 526 375
t: +61 7 3139 0325
e: micheal.axelsen@appliedinsight.com.au
blog: www.michealaxelsen.com

Applied Insight Pty Ltd
PO Box 603
Toowong DC 4066
AUSTRALIA



64



About the speaker



Services

- Micheal Axelsen provides consulting services in the enterprise governance of information technology, and the development and implementation of strategy to deal with the business challenges of information technology.

Position and qualifications

- Director of Applied Insight Pty Ltd
- Chair of CPA Australia Information Technology & Management Centre of Excellence
- Qualifications
 - Bachelor of Commerce (Hons)
 - Masters of Information Systems
 - FCPA

Appendices

Appendix: For further reference


65



Appendix:
For further reference



66



References

- AS/NZS 4360:2004 Risk Management
- Boyd, D., and Ellison, N. "Social Network Sites: Definition, History, and Scholarship," Journal of Computer-Mediated Communication (13:1), March 2007, pp 210-230.
- Brandenburg, C. 'The Newest Way to Screen Job Applicants: A Social Networker's Nightmare'. Federal Communications Law Journal. Los Angeles: Jun 2008. Vol. 60, Iss. 3; p. 597 (30 pages).
- Emerald Insights. 'MySpace or yours? Advertising and social networks'. Strategic Direction. Bradford. 2008. Vol. 24, Iss. 8; p. 15
- Engdahl, S (Editor). "Online social networking". Greenhaven Press. Farmington Hills, MI, USA. c2007.

67

 **References**

- Espejo, R (Editor). 'Should social networking web sites be banned?'. Greenhaven Press. Detroit, MI, USA. 2008.
- Johnson, R A, and Middleton, J M. 'Accounting for Second Life'. Journal of Accountancy. New York: Jun 2008. Vol. 205, Iss. 6; p. 54 (5 pages)
- Lavenda, D. 'Does 'blogging' have a place in the workplace?'. The British Journal of Administrative Management. Orpington: Jul 2008. p. 27 (3 pages)
- Mac Sithigh, D. 'The mass age of internet law'. Information & Communications Technology Law. Abingdon: Jun 2008. Vol. 17, Iss. 2; pg. 79
- McCallum, R. "Employer Controls over Private Life". New South Wales University Press Ltd. Sydney, NSW, Australia. 1999.

68

 **References**

- Stewart, A. 'Drafting and enforcing post-employment restraints'. Australian Journal of Labour Law. Vol 10 pp181-221. 1997.
- Willard, N E. 'Cyber-safe kids, cyber-savvy teens : helping young people learn to use the Internet safely and responsibly. Jossey-Bass. San Francisco, CA, USA. 2007.

Appendix: Developing your policy

69



Appendix:
Developing your policy



70



Tailoring your response

	Identify organizational context & risks	Analyse	Evaluate	Treat & Monitor
Objective	Identify the risks	Understand the risks	Evaluate the risks	Treat the risks
Key steps	<ul style="list-style-type: none"> Identify business strategy and market position Assessment of online presence Staff survey Stakeholder interviews Document risks 	<ul style="list-style-type: none"> Identify likelihood Identify consequences Risk evaluation workshop 	<ul style="list-style-type: none"> Evaluate risks and risk level to identify risks that require treatment Match risks to policy and procedure template to develop a policy 	<ul style="list-style-type: none"> Develop program of activities from procedures Establish monitoring program
Project Outputs	Identified risks	Estimated risk level	Online Social Networking Policy	Implemented policy & procedures

71

 Identify the risks

Identify business strategy and market position

- Identify organisational focus
- Identify organisational strategy and context

Assessment of online presence

- Online search for mentions of business name, key products, and senior management team.
- Social networking search for current and past employees.
- Search of relative subscriber-only forums not indexed by search engines.

72

 Identify the risks

Stakeholder survey

- A broad survey of stakeholders (including customers, business owners and staff) to identify the extent of participation in online social networking.
- Request suggestions on appropriate online behaviour from stakeholders

Stakeholder interviews

- Identify current activities, expectations of appropriate behaviour, and general attitude towards OSN

73

 Identify the risks

Document risks

- Review the information recorded above, and identify current and potential online social networking activities, and consider the potential risks that arise as a result of these actions.
- Consider the seven potential risks
- Document the risks, identifying online social networking activities that contribute to this risk.

74

Qi applied insight **Understand the risks**

Identify likelihood

- Have stakeholders rate the likelihood of each risk

Identify consequences

- Understand the risk and its impact
- Define levels of economic loss
- What is the consequence of each risk?
- Have stakeholders rate the consequences of each risk

75

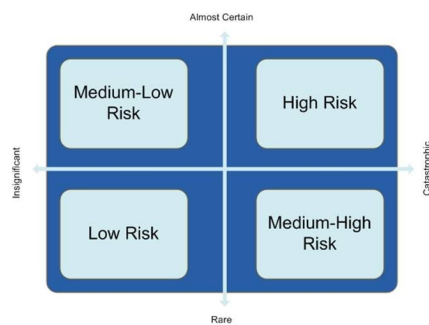
Qi applied insight **Understand the risks**

Risk evaluation workshop

- Use a workshop to agree on an estimated risk level
- Aggregate consequence assessment. Confirm in workshop.
- Map each risk to the matrix below
- Document the estimated risk level

76

Qi applied insight **Understand the risks**



77

Q
applied insight **Evaluate the risks**

Evaluate risks and risk level

- Identify the acceptable estimated risk level
- Assign each identified risk to the below matrix
- Identify non-policy activities or changes to work practices to:
 - avoid the risk
 - reduce the likelihood of its occurrence
 - to reduce its consequences
 - to transfer the risk to a third party.
- What remains is the residual risk that must be reduced through an online social networking policy

78

Q
applied insight **Evaluate the risks**

Estimated Risk Level	Avoid Risk	Reduce Likelihood	Reduce Consequences	Transfer Risk	Residual Risk Level
Legal (VLL/M/HVB)					(VLL/M/HVB)
Legal (VLL/M/HVB)					(VLL/M/HVB)
Reputation (VLL/M/HVB)					(VLL/M/HVB)
Viruses and Spyware (VLL/M/HVB)					(VLL/M/HVB)
Privacy breaches and identity theft (VLL/M/HVB)					(VLL/M/HVB)
Social engineering (VLL/M/HVB)					(VLL/M/HVB)
Inadvertent release of information (VLL/M/HVB)					(VLL/M/HVB)

79

Q
applied insight **Evaluate the risks**

Match risks to policy and procedure template

- Five core procedure responses, matched to your risk appetite:
 1. Acceptable online social networking activities
 2. Staff awareness program
 3. Staff training program
 4. Online reputation monitoring
 5. Responding to online social networking activities
- Provides a draft online social networking policy that can be developed further

Validation Check

- Refinement will be needed
- Circulate, discuss, and confirmed

80

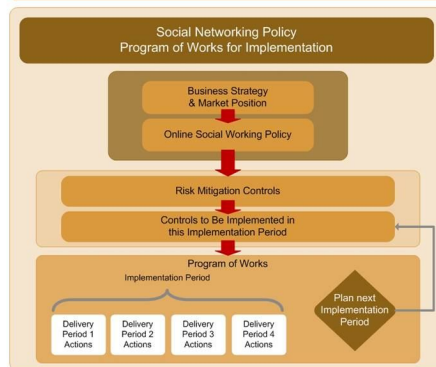
Qi applied insight **Treat and monitor**

Develop program of activities from procedures

- Steady and sure approach is usually best
- Three crucial factors:
 - Be realistic (and then halve it!)
 - Prioritise the identified risk mitigation controls with separate actions
 - Identify a program of work over the planning horizon period

81

Qi applied insight **Treat and monitor**



82

Qi applied insight **Treat and monitor**

Establish monitoring program

- Review actions each delivery period
- Plan the actions for delivery in the next
- Focus on the development of an active strategy
- Regularly monitor & review in a group
- Monitor effectiveness
- Review policy & procedures annually

Appendix: Online Social Networking Risk Examples


83



Appendix:
OSN Risk Examples



84



Scenarios


Productivity Losses

- Employees use social networking websites during work time to the detriment of business performance.

Legal risks

- As no policy explicitly states that email use is monitored by the employer, the employee brings an action for wrongful dismissal when dismissed for posting inappropriate content to an email forum.
- As no policy explicitly states that web use is actively monitored, it is difficult for a business to further investigate an employee who is suspected of posting details of an upcoming marketing program and product price list onto Wikipedia.

85



Scenarios

- A junior financial planner with an accounting firm provides taxation advice in a public forum using the firm's email address and with a signature including the firm's name. The advice is posted publicly, is relied upon by some readers who suffer a loss and subsequently bring an action against the accounting firm.

Reputation Risk

- A customer writes a blog post or video that is negative towards your product, service or staff.
- An employee writes a blog post or posts a video that is negative towards the company's product, service or staff.

86



Scenarios

- An employee writes a blog post or status update that places company secrets in the public domain using the business's equipment.
- An employee posts lewd photographs online in a public forum.
- A friend of an employee posts lewd material on the employee's public website or social networking page.
- Photographs of office functions depicting inappropriate behaviour are posted online by staff.
- Photographs of office functions depicting inappropriate behaviour are posted online by staff employed by the venue.

87



Scenarios

- An employee writes a blog post or posts a video that is derogatory to his or her colleagues or the firm's customers.
 - An ex-employee writes a blog post or posts a video that is derogatory to his or her colleagues or the firm's customers.
 - A supplier writes a blog post that is derogatory about the company's ability to pay its suppliers.
- Viruses & spyware**
- A staff member's computer infects all networked computers with a virus that was launched from a website that advertised on MySpace.

88



Scenarios

- The accountant's username and password for the business's online banking is stolen by a Trojan key-logging program that was downloaded to the accountant's laptop from an advertisement on a niche social networking website while her teenaged son was using the computer at home.
- Privacy breaches/identity theft**
- Using an edited copy of a signed letter and a business-card posted on Flickr, a fraudster creates a fake letter of employment as supporting documentation for a bank loan in an employee's name that is subsequently defaulted upon and causes personal bankruptcy for the employee.

89



Scenarios

- The employee subsequently brings an action against the business for not taking reasonable precautions to prevent this from happening. Although the resulting court case is unsuccessful, it is a serious distraction and expense for the business.
- An employee posts a photograph of a colleague and her children on her blog at the annual Christmas function. The colleague's estranged husband is able to identify the children's school from the uniform they are wearing, and subsequently collects the children from the school. The children are never seen again.

90



Scenarios

Social engineering

- Using names, email address, and positions gleaned from Facebook, position titles and references from LinkedIn, and faked letterhead or invoices from a site such as Flickr or Photobucket, a conman is able to extract payment for non-existent products or services.
- Using photos from Flickr of a business card and letterhead, and information gleaned from Facebook, a fraudster poses as a contract cleaner who then uses an unattended and logged-in computer to steal clients' taxation information on a 4gb USB memory stick.

91



Scenarios

Inadvertent release of information

- The company's proprietary approach to the bidding process for government work is submitted to Wikipedia by the business development assistant and is not able to be withdrawn in time.
